MyID

Version 10.8 Update 2 Revision 2

Release Notes

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Copyright

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:
  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning:	You must take a backup of your database before making any changes to it.

Contents

1 Introduction 9

1.1 Change history 9

1.2 Further information 9

1.3 PIV edition 10

2 Latest Updates 11

2.1 MyID 10.8 Update 2 Revision 2 11

2.1.1 Server core platform updates 11

2.2 MyID 10.8 Update 2 Revision 1 11

2.2.1 Support for TLS 1.2 11

2.2.2 Server core platform updates 12

3 Previously in MyID 10.8 Update 2 13

3.1 Card activation processes 13

3.2 Assisted Activation and Terms and Conditions 13

3.3 Using virtual smart cards as a backup on Windows 8.1 and 10 14

3.4 Credential policy enhancements 14

3.4.1 Validating replacement card jobs 14

3.4.2 Print quality confirmation in Collect Card 14

3.4.3 Enforce photo at card collection 14

3.5 Mobile credentials 15

3.5.1 Enhanced retries mechanism when collecting mobile credentials 15

3.5.2 Updates to mobile operating system support 15

3.5.3 Change PIN on Intercede mobile key store 15

3.5.4 Android fingerprint support 15

3.6 Technical enhancements 15

3.6.1 Support for Symantec (Digicert) MPKI v8 15

3.6.2 Updates to supported smart cards 16

3.6.3 Updates to HSM support 16

3.6.4 Updates to Windows operating system support 16

3.6.5 External prox readers 16

3.6.6 Updated import schemas for Lifecycle API 17

3.7 Tools and utilities 17

3.7.1 Audit Verifier 17

3.7.2 Patch Removal Utility 17

3.7.3 Password Change Tool 17

3.8 Previously issued patches incorporated to this release 17

3.9 Known issues resolved in MyID 10.8 Update 2 18

3.10 End of life features 19

3.10.1 Windows Phone 19

4 Previously in MyID 10.8 Update 1 20

4.1 Enhancements to Virtual Smart Card support 20

4.1.1 Issuing VSCs to TPMs with reduced functionality 20

4.1.2 Replacing Virtual Smart Cards 20

4.2 Mobile Device Management (MDM) System Integration 20

4.3 Additional features 20

4.3.1 Logon code complexity settings 20

4.3.2 Cancelling previously issued devices 21

4.3.3 Support for UniCERT UPI Certificate Authority 21

4.3.4 Mobile identity licenses 21

4.4 Technical enhancements 21

4.4.1 New name for VeriSign Certificate Authority 21

4.4.2 Configuring Integrated Windows Logon 21

4.4.3 .NET framework version 4.6 21

4.4.4 Mobile User role 21

4.4.5 Encoding spaces in email templates 22

4.5 Known issues resolved in MyID 10.8 Update 1 22

4.6 End of life features ... 22
4.6.1 Precise biometrics readers ... 22
5 Previously in MyID 10.8 ... 23
5.1 New workflows ... 23
5.1.1 Collect Card workflow ... 23
5.1.2 Batch Collect Card workflow ... 23
5.1.3 Mailing documents ... 23
5.1.4 Upgrading systems to use new workflows ... 23
5.2 Simple provisioning of certificates to Apple iOS devices ... 24
5.3 Support for Intel Virtual Smart Cards with Intel Authenticate ... 24
5.4 Additional features ... 24
5.4.1 Connecting to alternative MyID servers ... 24
5.4.2 Enhancements to role-based access control for credential management ... 24
5.4.3 Issuing key pairs to smart cards from new clients ... 25
5.4.4 System Interrogation Utility ... 25
5.4.5 Lifecycle API updates ... 25
5.4.6 Self-Service PIN change ... 25
5.5 Technical enhancements ... 26
5.5.1 Updates to supported smart cards ... 26
5.5.2 Windows Server 2016 ... 26
5.5.3 SQL Server Updates ... 26
5.5.4 SafeNet Assured Technologies Luna SA for Government ... 26
5.6 Known issues resolved in MyID 10.8 ... 26
5.7 End of life features ... 27
5.7.1 Physical signature option for Terms and Conditions. ... 27
5.7.2 Internet Explorer 9 and 10 ... 27
5.7.3 Windows 8 ... 27
5.7.4 Smart cards ... 27
6 Previously in MyID 10.7 Update 1 ... 29
6.1 Extended support for Elliptic Curve Cryptography ... 29
6.2 Support for Yubico YubiKey 4 devices ... 29
6.3 Updated support for SafeNet devices ... 29
6.4 Support for Gemalto PIV cards using SCP03 ... 29
6.5 Support for SQL Server 2016 ... 29
6.6 Mobile enhancements ... 29
6.7 Issued devices list in the System Status report ... 29
6.8 Known issues resolved in MyID 10.7 Update 1 ... 30
6.9 End of life features ... 30
6.9.1 SQL Server 2012 ... 30
6.9.2 SafeNet smart cards ... 30
7 Previously in MyID 10.7 ... 31
7.1 Intel Virtual Smart Cards ... 31
7.2 New workflows ... 31
7.2.1 Erase Card ... 31
7.2.2 Cancel Credential ... 31
7.2.3 Reset Card PIN ... 32
7.2.4 Unlock Credential ... 32
7.2.5 Print Card ... 32
7.2.6 Upgrading systems to use new workflows ... 32
7.2.7 Searching for people in the new workflows ... 33
7.3 Import and distribute certificates to devices ... 33
7.4 Temporary Virtual Smart Cards ... 33
7.5 Microsoft Azure ... 34
7.6 Mobile enhancements ... 34
7.7 Additional features ... 34
7.7.1 ECC support ... 34
7.7.2 Enhanced automatic key recovery at certificate renewal ... 34
7.7.3 Bureau issuance ... 35

7.7.4 Fargo HDP 8500 ... 35
7.7.5 Additional Identities API ... 35
7.7.6 Assigning cards ... 35
7.7.7 Email PIN option ... 35
7.7.8 Customizing terms and conditions ... 35
7.7.9 Allow self requests option ... 36
7.7.10 Activation and unlock options for MyID Desktop ... 36
7.7.11 Request External Certificates workflow ... 36
7.8 Technical enhancements ... 36
7.8.1 Document scanning ... 36
7.8.2 Enhancements to data model storage location ... 36
7.8.3 Web service user ... 37
7.8.4 COM+ encryption ... 37
7.8.5 Editing Certificate Authority details ... 37
7.8.6 Storing HSM PINs ... 37
7.8.7 Stored procedure for sending SMS ... 37
7.9 End of life features ... 38
7.9.1 Replaced web operations ... 38
7.9.2 Support for TWAIN drivers when scanning documents ... 38
7.9.3 Server-generated Virtual Smart Card ... 38
7.10 Known Issues resolved in MyID 10.7 ... 38
8 Previously in MyID 10.6 Update 1 ... 40
8.1 Configurable number of security questions for authentication ... 40
8.2 Configuring authentication for unlocking ... 40
8.2.1 Upgrading existing systems ... 40
8.3 Configuring authentication for mobile unlocking ... 40
8.4 LDAP update ... 41
8.5 Launching MyID Desktop with automatic Windows Logon ... 41
8.6 Unlock My Security Phrases workflow ... 41
8.7 Wildcard serial number search in Request Card ... 41
8.8 Controlling the visibility of device history tabs ... 42
8.9 Unrestricted cancelation ... 42
9 Previously in MyID 10.6 ... 43
9.1 Updated user interface ... 43
9.2 Enhanced email capability ... 43
9.3 Signed email notifications ... 43
9.4 Mobile identities ... 44
9.5 Enhanced HSM Test Utility ... 44
9.6 Client Components version options ... 44
9.7 Database names in email messages ... 44
9.8 Logon Name Required option ... 44
9.9 Mobile identity management changes ... 45
10 Previously in MyID 10.5 ... 46
10.1 Automated certificate updates across devices ... 46
10.2 Certificate configuration updates ... 46
10.2.1 Selecting certificates in credential profiles ... 46
10.2.2 Certificate configuration options ... 46
10.3 Enhanced credential updates ... 47
10.4 Support for Windows 10 ... 47
10.5 Enhanced PIN policy rules ... 47
10.6 Microsoft Virtual Smart Card (VSC) improvements ... 47
10.7 Additional updates ... 47
10.8 Email credential PIN at issuance ... 48
11 Previously in MyID 10.4 ... 49
11.1 Enhancements to Microsoft Virtual Smart Card support ... 49

11.2 Additional identities 49
11.3 Windows Integrated Logon 49
11.4 Control which roles can validate credential requests 50
11.5 HSM concurrency support 50
11.6 AES256 master keys 50
11.7 VSC priority when collecting jobs in the Self-Service App 50
11.8 End of life features 51
11.8.1 Removal of Abort On Failure? option 51
12 Previously in MyID 10.3 52
12.1 Enhanced security features 52
12.2 Simple Certificate Enrollment Protocol (SCEP) 52
12.3 Simplified self-service smart card issuance 52
12.3.1 Logon codes 52
12.3.2 Launching new clients using a hyperlink or command line 53
12.4 Improved Batch Directory Synchronization Tool 53
12.5 Default roles and inheriting roles 53
12.6 Restricting data returned in a Management Information Report 53
12.7 Certificate management for TPM based devices 54
12.8 Enhanced support for Entrust Certificate Authority 54
12.9 Support for Thales nCipher PCI HSM 54
12.10 eDB Data Import Server 54
13 Previously in MyID 10.2 55
13.1 MyID Desktop 55
13.2 Licensing changes 55
13.3 Increased security for security phrases 55
13.4 Support for derived credentials 55
13.5 Associating LDAP groups with MyID roles 55
13.6 Tracking users when their OU is changed in the LDAP 56
13.7 Active Directory Deletion Tool 56
13.8 Specifying a certificate store in Microsoft CAs 56
13.9 Increased length of email templates 56
13.10 Recovering archived certificates 56
13.11 Reporting API web service 56
14 Previously in MyID 10.1 57
14.1 MyID Desktop 57
14.2 Support for SQL Server 2014 57
14.3 Key Recovery 57
14.4 Device Identities 57
14.5 Updated HSM support 58
14.6 Unlock Card validation 58
14.7 Authenticating users 58
14.8 Disposing of cards 58
14.9 Improved envelope mechanism 59
14.10 Mobile identities 59
15 Previously in MyID 10.0 61
15.1 Installation program 61
15.2 Unique IDs for audit information and certificates 61
15.3 Device identities 61
15.4 Mobile identities 61
15.5 Microsoft Virtual Smart Cards 62
15.6 Self-Service applications 62
15.7 PIV card support 62

15.8 Updated printer support 62
15.9 Global key recovery 62
15.10 File storage in the database 62
15.11 Terminology updates 63
15.12 Combination of documentation 63
15.13 End of life features 63
15.13.1 Online help 63
15.13.2 List Devices workflows 63
15.13.3 MIFARE 63
15.13.4 Import from file 63
15.13.5 SMTP email 63
15.13.6 Smart card support in GenMaster 63
15.13.7 Soft certificates 64
15.13.8 Request and collect certificate recovery 64
15.13.9 Windows XP for client PCs 64

16 Previously in Mobile Releases 65
16.1.1 MOB-10.5.1000.1 65
16.1.2 MOB-10.4.1000.1 65
16.1.3 MOB-10.3.1000.2 66
16.1.4 MOB-10.3.1000.1 66
16.1.5 MOB-10.1.1000.2 66
16.1.6 MOB-10.1.1000.1 66
16.1.7 MOB-10.0.1000.5 66
16.1.8 MOB-10.0.1000.4 67
16.1.9 MOB-10.0.1000.2 67
16.1.10 MOB-10.0.1000.1 67

17 Known Issues 68

1 Introduction

This document describes changes made to MyID® in version 10.8 Update 2 Revision 2. This release provides new and updated features.

1.1 Change history

Version	Description
IMP1749-01	First release with MyID 10.0.
IMP1749-02	Minor corrections and updates to the following documents: Installation and Configuration Guide Microsoft Windows CA Integration Guide SafeNet LUNA SA HSM Integration Guide
IMP1749-03	Release with MyID 10.1.
IMP1749-04	Release with MyID 10.2
IMP1749-05	Minor updates immediately prior to the release of MyID 10.2.
IMP1749-06	Release with MyID 10.3.
IMP1749-07	Release with updated version of MyID 10.3.
IMP1749-08	Release with MyID 10.4.
IMP1749-09	Release with MyID 10.5.
IMP1749-10	Release with MyID 10.6.
IMP1749-11	Release with MyID 10.6 Update 1.
IMP1749-12	Release with MyID 10.7.
IMP1749-13	Release with MyID 10.7 Update 1.
IMP1749-14	Release with MyID 10.8.
IMP1749-15	Release with MyID 10.8 Update 1.
IMP1749-16	Release with MyID 10.8 Update 2.
IMP1749-17	Release with MyID 10.8 Update 2 Revision 1.
IMP1749-18	Release with MyID 10.8 Update 2 Revision 2.

1.2 Further information

The ***Getting Started*** document provides an overview of the main components, clients, tools, and utilities provided with MyID and where to locate them in the release media.

The ***Installation and Configuration Guide*** provides details of the hardware and software requirements, implementation decisions, installation procedure, and post-installation configuration of your MyID software.

The ***Administration Guide*** provides procedures for configuring, administering, and using MyID to request, issue, and manage identity credentials for your users.

The ***System Security Checklist*** provides important information on making sure that your system takes full advantage of the security technology provided with MyID.

The HSM integration guides provide information on setting up your HSM to secure your MyID system.

The PKI integration guides provide information on setting up your certificate authorities.

The MyID client components guides – the ***Client Components Release Notes***, ***Printer Integration Guide***, and ***Smart Card Integration Guide*** – provide information on setting up your MyID clients, printers, and smart cards.

1.3 PIV edition

MyID is available in a core edition and a PIV edition, which provides support for compliance with FIPS 201-2. For details of the PIV-specific features in this release, see the ***PIV Release Notes***, which is provided with the PIV edition of MyID.

The features described in this document are also applicable to the PIV edition, unless otherwise stated.

2 Latest Updates

2.1 MyID 10.8 Update 2 Revision 2

2.1.1 Server core platform updates

This revision contains the following additional update in the `Server Core Platform Updates` folder; you must install all of the updates to ensure that your installation is fully up-to-date:

- VTEN-10.8.1000.204 – Updated support for Symantec MPKI.

  This patch provides a mandatory update that is essential for Symantec MPKI support.

  This patch includes the following features:

  - Support Cloud and Enterprise escrow on MPKI 8.
  - Provide instructions for mapping the `seat_id`.
  - Address an issue with MPKI 7 systems unexpectedly reporting A506 (missing NVP) error.

  See the updated ***Symantec (Digicert) Managed PKI Integration Guide***.

2.2 MyID 10.8 Update 2 Revision 1

2.2.1 Support for TLS 1.2

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network. SSL is now deprecated and replaced by TLS. The initial version, TLS 1.0, is now no longer recommended for use under some security policies, but certain Microsoft components used by MyID still require the use of TLS 1.0.

This revision provides instructions on configuring MyID to support TLS 1.2. For more information, see the *Web Site Security* and *Database Security* sections in the ***System Security Checklist***.

The VTEN-10.8.1000.201 and MWS-3.2.1000.2 installation programs provided in this release have also been updated to support TLS 1.2, and therefore require SQL Server Native Client version 11 to be installed. Note, however, that all previous MyID installation programs, including the main product installation program, do *not* support TLS 1.2; before running any of these installation programs, you must re-enable TLS 1.0. After completing the installation, you can disable TLS 1.0 again.

2.2.2 Server core platform updates

This revision contains the following additional updates in the `Server Core Platform Updates` folder; you must install these updates to ensure that your installation is fully up-to-date:

- VTEN-10.8.1000.201 – Email notification enhancements.

  This patch provides enhancements to the MyID notifications system to support the generation of email notifications when devices are cancelled, disabled, or enabled. The patch provides the following:

  - New email notification that can be triggered when a device is cancelled.
  - New email notification that can be triggered when a device is disabled.
  - New email notification that can be triggered when a device is enabled.

  The patch also addresses an issue that prevented the revocation comment entered into the **Details** field in the **Enable / Disable Card** workflow from being recorded against the device that was being disabled.

  This patch installation program supports TLS 1.2.

- MWS-3.2.1000.2 – Web Services Architecture.

  This patch provides the following new feature:

  - Improved handling for tracking certificates during multiple rejected activation attempts.

  This patch installation program supports TLS 1.2.

3 Previously in MyID 10.8 Update 2

3.1 Card activation processes

Issuing, personalizing, and securely distributing smart cards can be challenging for large enterprises with distributed offices and locations, where having on-site card printing facilities is not possible.

Secure card activation processes, previously only available in MyID PIV, are now available for all smart card and token types supported by MyID. This enables cards to be centrally produced with a randomized locked user PIN and then distributed to end users along with a printed letter or email providing details of how to activate the card. The card is also secured with a randomized security officer PIN and diversified global platform keys (where supported by the card type). The notification includes a unique one-time-code for activating the card.

The card can be activated by the user themselves, using MyID. They are guided through the activation process, including authentication using the one-time-code, displaying and recording acceptance of terms and conditions information where required and allowing the user to set the PIN.

Sometimes, the user may not be able to complete self-service activation. The **Assisted** Activation workflow allows an authenticated MyID operator to help the user activate their card, including authenticating the user.

See the ***Administration Guide*** for details of the activation process.

3.2 Assisted Activation and Terms and Conditions

The **Assisted Activation** workflow has been replaced as part of the migration away from Internet Explorer-based workflows. It also provides more flexibility with authentication options when activating the card and uses a new system for displaying HTML format terms and conditions that the cardholder must accept before the card is activated.

You can create multiple templates for the terms and conditions text, and store them in the MyID database. You then associate the template with the credential profile; this allows you to use different templates for different types of card.

Note: The **Assisted Activation** workflow replaces the previous version; however, for backwards compatibility the previous version has not been removed. You must update your role assignments to include the new **Assisted Activation** workflow. If you hover your mouse over the name of the workflow, you will see the supported clients; the new workflow is supported on "MyID Desktop", while the previous workflow is supported only on "Desktop Client (Web UI)" legacy systems.

See the ***Administration Guide*** for details.

3.3 Using virtual smart cards as a backup on Windows 8.1 and 10

MyID has the capability to issue a backup to a physical smart card in the form of a locked virtual smart card to a device. If an end user does not have access to their physical smart card, this virtual smart card can be unlocked, providing the user access to services without the organization having to resort to less secure authentication mechanisms.

The VSC can be unlocked for a limited period of time. Once this period has elapsed, or if the user's physical smart card is re-enabled earlier, the VSC will be automatically locked when the computer next connects to MyID.

This feature was previously only available on Windows 7, and has now been extended to support Windows 8.1 and Windows 10.

See the ***Microsoft Virtual Smart Card Integration Guide*** for details.

3.4 Credential policy enhancements

3.4.1 Validating replacement card jobs

The **Approve Replacement Cards** configuration option (on the **Process** page of the **Security Settings** workflow) has been extended to allow a third option. In addition to **Yes** (all replacement cards require validation) and **No** (no replacement cards require validation), you can now select **Ask**, which will require validation for a replacement card only if the credential profile has the **Validate Issuance** option set.

If you do not set the **Approve Replacement Cards** option to **Ask**, the **Validate Issuance** option in the credential profile has no effect on replacement cards; it is used for initial card issuance only.

See the ***Administration Guide*** for details.

3.4.2 Print quality confirmation in Collect Card

You can now configure MyID to ask the operator to confirm that a card printed correctly using the **Collect Card** workflow, and offer an opportunity to retry the operation. Set the **Print Quality Confirmation** option on the **Devices** tab of the **Operation Settings** workflow.

See the ***Administration Guide*** for details.

3.4.3 Enforce photo at card collection

The **Enforce Photo at Issuance** option has been updated. Previously, this was a checkbox; when selected, it prevented credentials from being requested if a photo of the cardholder was not present in MyID.

Now, there are three options:

- **No** – you can issue cards if the cardholder does not have a photo.
- **Request and Issuance** – you cannot request or issue a card if the cardholder does not have a photo.

  This state is the equivalent of the original **Checked** state.
- **At Issuance Only** – you can request a card, but if the cardholder does not have a photo you will be unable to issue or activate the card.

See the ***Administration Guide*** for details.

3.5 Mobile credentials

3.5.1 Enhanced retries mechanism when collecting mobile credentials

MyID has been enhanced to support multiple retries when collecting a credential on a mobile device, which improves reliability and resilience on slow or non-responsive network connections.

See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

3.5.2 Updates to mobile operating system support

MyID now supports:

- MobileIron integration on iOS 11.
- Android O support across mobile apps and SDKs.
- iOS 11 support across mobile apps and SDKs.

See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

3.5.3 Change PIN on Intercede mobile key store

Where the Intercede mobile key store is used, this feature gives the end user the ability to change the PIN used to protect the credentials in the store.

Change PIN is a feature available in the MyID Identity Agent app, which is available from the Apple App Store or Google Play.

3.5.4 Android fingerprint support

The MyID Mobile SDK now supports the use of fingerprint authentication on suitably enabled Android devices.

The SDK is available on request from Intercede.

3.6 Technical enhancements

3.6.1 Support for Symantec (Digicert) MPKI v8

MyID now supports certificate issuance and key recovery capabilities with Symantec Managed PKI Service v8.

Note: Following the acquisition of Symantec PKI solutions by Digicert, there may be differences in the branding of documentation and information supplied to you by Digicert when compared to MyID. Throughout MyID, the brand name Symantec is used in user interface and lower level components. This approach has been taken to avoid backwards compatibility issues for customers who are upgrading from earlier product versions.

See the ***Symantec (Digicert) Managed PKI*** integration guide for details.

3.6.2 Updates to supported smart cards

The following smart cards and tokens are now supported in this release:

- Idemia (Oberthur) v8.1 card with v2.4.1 PIV applet
- Gemalto ID Prime PIV v2.1 applet on TOP DL v2.1 card platform
- Giesecke & Devrient (G&D) SCE 7.0 PIV card
- Gemalto ID Prime MD831 cards
- Gemalto Minidriver v8.5.0.7 (used with ID Prime MD smart cards)
- SafeNet eToken 5110 FIPS
- SafeNet authentication client v10.4 (used with SafeNet eTokens)
- IDProtect Client 7.1.2.7 (used with Athena ID Protect and TicTok smart cards)

Oberthur and IDEMIA smart cards

The Oberthur section of the ***Smart Card Integration Guide*** has been renamed IDEMIA to align with the change of name by the card manufacturer. Existing smart cards are still named Oberthur ID-One; internal references within MyID will continue to state the device name as Oberthur.

See the ***Smart Card Integration Guide*** for details.

3.6.3 Updates to HSM support

MyID has now been tested with the following HSM versions

- Thales nShield HSM (client versions 12.20.00 and 12.20.50)
- SafeNet network HSM v7

3.6.4 Updates to Windows operating system support

MyID clients have now been verified on:

- Windows 10 version 1709 (Fall creators update)

See the ***Installation and Configuration Guide*** for details

3.6.5 External prox readers

You can use the **Printers have External Prox** Readers option (on the **General** tab of the **Operation Settings** workflow) to configure MyID to ask the operator to read the proximity serial number using an external prox reader before inserting the card into the printer when using the **Collect Card** workflow.

See the ***Administration Guide*** for details.

3.6.6 Updated import schemas for Lifecycle API

You can use the Lifecycle API to import user data to MyID, make requests for credentials, and to perform lifecycle management functions for credentials. This release includes updated core import schemas for MyID, including the following changes:

- Middle name field is extended to 50 characters.
- New `CardLayout` node.
- `SerialNumber` and `DeviceType` nodes for targeted issuance now available for PIV as well as CMS.
- Parameters for PIV and CMS schemas updated to be the same.
- New `ReplaceUnassignedCards` parameter.
- Updated list of hair colors in the PIV schema.

If you are using a customized import schema, you may need to make modifications to your current schema and configuration of the Lifecycle API to continue using it. Details of the amended schemas, and how to configure the API to use a customized schema are provided in the Lifecycle API document – you can find this in the APIs folder in the release.

The updated core schemas must be added separately to your installation. To install these, use the installer provided in the Custom Lifecycle Schema Enabler in the APIs folder of the MyID release.

3.7 Tools and utilities

3.7.1 Audit Verifier

MyID maintains a signed audit record of events, but it can be difficult to verify that the audit records are valid and have not been tampered with.

The audit verifier tool is a simple utility that will allow you to verify the integrity of MyID audit data.

You can find this utility in the Support Tools folder.

3.7.2 Patch Removal Utility

Before upgrading MyID, in some cases, you may need to remove earlier patches from the installation. PowerShell scripts are provided to allow you to automate this step.

You can find this utility in the Support Tools folder.

3.7.3 Password Change Tool

MyID uses Windows service accounts to provide security context between components and server tiers in a MyID installation. The Password Change Tool (PCT) is a support tool for automating the changing of passwords for the accounts used by MyID. You are recommended to use it if MyID is already installed and you are required to change passwords regularly by your security policy, or if a security breach has occurred.

You can find this utility in the Support Tools folder.

3.8 Previously issued patches incorporated to this release

This product release incorporates the following patches that may have previously been provided separately:

- VTEN-10.8.1000.6

  - v10.8 Update 1 release.
- VTEN-10.8.1000.7
  - Enable Key Ceremony for PIV Smart Card 9B Keys when no HSM is in use.
  - Prevent duplicate FASCN generation for non-federal PIV cards.
- VTEN-10.8.1000.9
  - Addresses an issue that prevented jobs being collected using the Self-Service App.
- VTEN-10.8.1000.10
  - Support for Oberthur v8 cards that need to be imported with a Prox correlation file.
- VTEN-10.8.1000.12
  - Addresses an issue where a logon message stating "Your System Is Not Configured For Production" was displayed.
- VTEN-10.8.1000.13
  - Provides an essential fix for Symantec MPKI support after MyID 10.8 Update 1 has been installed.
- VTEN-10.8.1000.14/VTEN-10.8.1000.16
  - Credential policy enhancements – see section *3.4*, *Credential policy enhancements*.
- VTEN-10.8.1000.19
  - Fix to allow Windows logon with devices using a CIV data model.
- VTEN-10.8.1000.21
  - Update to make `EmployeeAssociation` mandatory when importing users using the `PIVXMLWebImport` method of the Lifecycle API.
  - Fix to use the latest credential profile when reprovisioning a card, rather than the credential profile that was originally used to issue the credential.
  - Reprovision of Enterprise cards using a PIV data model.

3.9 Known issues resolved in MyID 10.8 Update 2

The following known issues have been resolved in the current version of MyID:

- IKB-82 – Historic Certificates not supported on Windows Phone
- IKB-112 – Invalid Credential Profile error with disabled certificate policies
- IKB-161 – SMS links may not be recognized in some versions of Windows 10 Mobile
- IKB-164 – Intermittent error when recovering a certificate to a Microsoft Virtual Smart Card

  The issue was reported to Microsoft, and has been resolved in Windows 10 Anniversary update. The required minimum Windows 10 version is 1607 (OS build 14393).
- IKB-178 – Cannot log on to Windows with Oberthur ID-One PIV (v2.4.0) or IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1
- IKB-205 – Removed certificates are reported as unsuspended
- IKB-208 – Cannot change PIN when certain symbols are used

- IKB-211 – Memory problems with Gemalto minidriver-based cards
- IKB-214 – ECC certificates not displayed in Identify Card workflow
- IKB-217 – Issues with Athena minidriver

  This error is resolved when using the 7.1.2.7 version of the minidriver.
- IKB-223 – Error when collecting dual interface smart cards using a printer

3.10 End of life features

3.10.1 Windows Phone

MyID no longer supports Windows Phone 8.1 or Windows Phone 10. Customers upgrading from previous versions of MyID who continue to require support for these devices should contact Intercede customer support for further guidance quoting SUP-49.

4 Previously in MyID 10.8 Update 1

4.1 Enhancements to Virtual Smart Card support

4.1.1 Issuing VSCs to TPMs with reduced functionality

In previous releases of MyID, creating a VSC has required that the trusted platform module reports its status as "IsReady" to MyID, showing it is fully operational.

Under some circumstances, the TPM status may be reported as:

```
"The TPM is ready for use, with reduced functionality."
```

This may occur when the TPM password is no longer known to the client PC. You must make sure that the password is stored somewhere else; for example Active Directory or BitLocker.

You can configure MyID to issue Microsoft VSCs when the TPM status is "reduced functionality" using the **Allow virtual smart card creation with TPM reduced functionality** configuration option. See the ***Microsoft Virtual Smart Card Integration Guide*** for details.

4.1.2 Replacing Virtual Smart Cards

The collection process for VSCs has been improved to remove any previously issued virtual smart cards for the current user, that are now revoked. This ensures that only the latest credentials are available on the computer.

4.2 Mobile Device Management (MDM) System Integration

MyID has been capable of issuing credentials (key and certificates) to mobile devices for several years. A key feature of MyID 10.8 Update 1 is out-of-the-box integration with a range of market leading Mobile Device Management (MDM) vendors including VMware AirWatch®, Citrix® XenMobile and MobileIron.

The integration allows MyID to write credentials into an MDM key store, enabling the MDM to use them for securing access to apps, data and services. The close integration, built in collaboration with each MDM vendor, allows credential issuance to be combined with device enrolment, providing a frictionless experience for end users.

See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

4.3 Additional features

4.3.1 Logon code complexity settings

You can now control the complexity of the logon codes generated by MyID.

When you set the **Generate Logon Code** option, you can now select one of the following options:

- **None** – no logon code is generated.
- **Simple** – the logon code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option.
- **Complex** – the logon code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option.

See the ***Administration Guide*** for details of setting up the complexity rules.

If you upgrade an existing system, any credential profile that previously had the **Generate Logon Code** option selected will default to **Complex**.

4.3.2 Cancelling previously issued devices

If you set the **Cancel Previously Issued Device** option on a credential profile, instead of *disabling* any previously-issued device because of the action of the **Active credential profiles per person** configuration option and **Credential Group** setting in the credential profile, MyID *cancels* the previously-issued devices.

4.3.3 Support for UniCERT UPI Certificate Authority

MyID now supports the UniCERT UPI Certificate Authority v5.4.1.

See the ***UniCERT UPI CA Integration Guide*** for details.

4.3.4 Mobile identity licenses

Issuing a mobile identity with certificates in multiple key stores no longer consumes a MyID credential license for each key store; only one license is now used for the mobile identity.

4.4 Technical enhancements

4.4.1 New name for VeriSign Certificate Authority

The Certificate Authority previously known as "VeriSign" is now the Symantec Certificate Authority.

See the ***Symantec MPKI Certificate Authority Integration Guide*** for details.

4.4.2 Configuring Integrated Windows Logon

This release updates the way MyID determines a user's domain name from their directory record. This means that you no longer need to set the **Force NETBIOS Name** configuration option.

See the ***Administration Guide*** for details of configuring Integrated Windows Logon.

If you set up MyID for Integrated Windows Logon, and have existing user accounts in MyID that were already imported before you installed this release, you may have to resynchronize the user records before you can use those accounts with Integrated Windows Logon.

You can do this by selecting the user account in the **Edit Person** workflow, or by using the Batch Directory Synchronization Tool. See the ***Administration Guide*** for details.

4.4.3 .NET framework version 4.6

MyID now requires .NET framework 4.6. This is required for MyID Desktop, Self-Service App, and Self-Service Kiosk. For server installations, you must install .NET Framework 4.6 before upgrading to MyID 10.8 Update 1.

See the ***Installation and Configuration Guide*** for details.

4.4.4 Mobile User role

The Mobile User role, as used for mobile identities, has been renamed to Server Credentials. See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

4.4.5 Encoding spaces in email templates

If an email template parameter value contains spaces (for example, a logon name) and you are using the parameter to build a URL (which does not allow spaces), you can use the following syntax to replace any spaces with + signs:

```
{%parameter:URI}
```

For example, `{%logonName:URI}` might become `Jane+Smith`.

As a complementary change, the Self-Service App now decodes usernames on the command line (whether from the Windows command line, or from a hyperlink) as URI-encoded; for example, `Jane+Smith` is treated as `Jane Smith`, with a space.

4.5 Known issues resolved in MyID 10.8 Update 1

The following known issues have been resolved in the current version of MyID:

- IKB-186 – Support for Charismathics PIV applets in MyID 10.7.
- IKB-195 – General upgrading issues.
- IKB-221 – Support for Windows 7 Virtual Smart Cards.

4.6 End of life features

4.6.1 Precise biometrics readers

The Precise 250 fingerprint reader is a legacy device that is no longer manufactured, and has not been tested with MyID from version 10.8 onwards.

5 Previously in MyID 10.8

5.1 New workflows

This release of MyID includes new workflows within MyID Desktop. This continues the migration away from using embedded Internet Explorer-based workflows.

5.1.1 Collect Card workflow

The **Collect Card** workflow has been completely updated for this release. This workflow allows collection of credential requests to a range of supported smart cards, incorporating electronic personalization, PIV personalization, certificate issuance, card surface printing and proximity-loop checks.

See the ***Administration Guide*** for details of using this workflow.

5.1.2 Batch Collect Card workflow

The **Batch Issue Card** workflow has been replaced by the **Batch Collect Card** workflow for this release. Using the capabilities of the new **Collect Card** workflow, it enables credential requests to be collected using a smart card printer with a hopper, automating production of large volumes of cards.

See the ***Administration Guide*** for details of using this workflow.

5.1.3 Mailing documents

The **Collect Card** and **Batch Collect Card** workflows use a new system to generate mailing documents. Instead of locally-stored Microsoft Word mail merge templates, MyID now uses centrally-stored HTML templates from the MyID database.

For information about setting up these templates, contact customer support quoting reference SUP-255.

5.1.4 Upgrading systems to use new workflows

MyID 10.8 introduces the following workflows:

- **Collect Card** – replaces the old **Collect Card** workflow.
- **Batch Collect Card** – replaces the old **Batch Issue Card** workflow.

To use these new workflows, you *must* use the latest MyID Desktop clients. If you do not upgrade MyID Desktop to the latest version, you will still be able to use the old versions of the workflows, but the new workflows will not appear in your list of available workflows.

You must use the **Edit Roles** workflow to provide permissions to the new workflows. You will then be able to use the new workflows; note, however, that you will no longer be able to see or use the old, replaced workflows.

For more information on upgrading to the new workflows, contact customer support quoting reference SUP-238.

Intercede understands that for large enterprises, deploying new clients can take time, and is therefore maintaining support for the old workflows (when used with the older versions of MyID Desktop or the web user interface) as described above.

This is intended to give customers time to update their clients, and customers should expect that over time support for the old workflows will be dropped.

5.2 Simple provisioning of certificates to Apple iOS devices

You can configure MyID to enroll a certificate on your iOS device using Over the Air (OTA) provisioning. The update appears on the device as a profile to be installed when you are issuing a mobile identity.

This feature requires the following additional web service modules to be installed and configured on your MyID server:

- SCEP – Simple Certificate Enrollment Protocol (SCEP) device identities
- IOSOTA – OTA (Over The Air) provisioning of certificates to iOS

See the ***Mobile Identity Management Installation and Configuration Guide*** for details.

The SCEP module is available in the APIs folder on the product CD, and the IOSOTA module is available in the Mobile folder on the product CD.

5.3 Support for Intel Virtual Smart Cards with Intel Authenticate

MyID can now issue and manage Virtual Smart Cards for use with Intel Authenticate as well as Intel IPT-PKI.

Intel Authenticate is a hardware-enhanced identity protection solution that delivers customizable multifactor authentication options, available on select 6th and 7th generation Intel® Core™ vPro™ platforms.

MyID manages the issuance process and provides lifecycle management for replacing or renewing credentials protected by Intel Authenticate.

Virtual Smart Cards can be managed alongside physical smart cards and mobile devices from the same installation.

See the ***Intel Virtual Smart Card Integration Guide*** for details of configuring MyID for either type of Intel VSC.

5.4 Additional features

5.4.1 Connecting to alternative MyID servers

MyID Desktop can now be redirected to other MyID servers. This allows administrators to switch between server environments; for example, test and production systems, or backup servers where network redirection is not available.

The available servers are limited to those whitelisted for use within the desktop client configuration.

See the ***Installation and Configuration Guide*** for details.

5.4.2 Enhancements to role-based access control for credential management

MyID controls access to credentials based on the roles assigned to each user account. Permissions for issuance and management of those credential types are also controlled using roles – for example which roles may validate requests for credentials. In this release, the following changes have been made:

- **Can Issue** – this option has been renamed to **Can Request** to reflect its use better. There are no functional changes.
- **Can Collect** – this permission controls which user accounts can collect credential requests.
- **Can Unlock** – this permission controls which user accounts can unlock or reset card PINs.

See the ***Administration Guide*** for details.

5.4.3 Issuing key pairs to smart cards from new clients

Cryptographic key pairs (without an associated certificate) can be used for logon and operator signing of transactions within MyID clients. The capability has previously existed with the web client, but can now be used with MyID Desktop. Card personalization processes in MyID Desktop and the Self-Service App can create key pairs on compatible cards.

See the ***Administration Guide*** for details of configuring credential profiles to support this capability, and the ***Smart Card Integration Guide*** for supported card types.

5.4.4 System Interrogation Utility

The System Interrogation Utility provides a simple method for checking configuration and operation of the MyID servers. This utility validates server configuration; for example, checking that correct prerequisites are installed and MyID server components can be launched.

This utility and instructions for its use can be found in the Support Tools folder on the MyID CD.

5.4.5 Lifecycle API updates

The Lifecycle API has been updated to allow `SerialNumber` and `DeviceType` nodes for targeted issuance; this allows smart cards to be pre-assigned to a user by an external system.

The `ReplaceUnassignedCards` parameter allows MyID to create a replacement request for a smart card that has previously been cancelled and unassigned from a user. For example, this can be used when a MyID workflow triggers cancellation of a card, but replacement requests are made using the Lifecycle API.

5.4.6 Self-Service PIN change

At MyID 10.7, the **Reset Card PIN** workflow was introduced to provide an operator-led process for managing card PINs, incorporating user authentication. This workflow does not provide a self-service capability for PIN change or unlock.

The **Reset PIN** option, accessed from MyID Desktop logon screen, requires additional authentication – for example an authentication code, security question, or fingerprint to verify the cardholder's identity before allowing the PIN to be reset.

The **Change PIN** workflow can be re-enabled in this release to allow self-service PIN change to take place without the requirement for additional authentication. The person using the workflow must know the current card PIN – no other restrictions are applied, and any card issued by MyID can have its PIN changed. The feature is available after logging in to MyID Desktop.

To enable **Change PIN** workflow, you need an additional update to MyID. Contact customer support for further information quoting SUP-262.

You can also carry out self-service PIN change by:

- Using the built-in Windows capability accessed through Ctrl-Alt-Delete.
- For smart cards that use a middleware supplied by the card manufacturer, using the capability built into the middleware user interface.
- For PIV cards, using the MyID Card Utility. This also incorporates challenge/response unlock capability.

5.5 Technical enhancements

5.5.1 Updates to supported smart cards

The following devices are now supported with this release

- SafeNet Assured Technologies SC650v4.1
- Yubico Yubikey Nano
- TickTok v2
- Gemalto MD830 Revision B

If you intend to use Charismathics PIV applets with MyID, contact customer support quoting SUP-54 for further information.

5.5.2 Windows Server 2016

MyID now supports Windows Server 2016 as a server platform. See the ***Installation and Configuration Guide*** for details.

5.5.3 SQL Server Updates

MyID has been tested with the following SQL Server versions

- SQL Server 2016 SP1 – CU1 for 2016 SP1 (13.0.4411.0 – January 2017)
- SQL Server 2014 SP2 – CU4 for 2014 SP2 (12.0.5540.0 – February 2017)
- SQL Server 2012 SP3 – CU7 for 2012 SP3 (11.0.6579.0 – January 2017)

Note: Intercede recommend using the database versions listed above. If you are going to use alternative service pack or cumulative update versions, make sure that you carry out additional testing within your environment.

5.5.4 SafeNet Assured Technologies Luna SA for Government

MyID now supports the SafeNet Assured Technologies Luna SA for Government configuration, and has been tested on the following system:

- A SafeNet Luna SA 5.4.7-3 running firmware version 6.21.2 or 6.10.9 using the v5.4.1 version of the SafeNet client software.

5.6 Known issues resolved in MyID 10.8

The following known issues have been resolved in the current version of MyID:

- IKB-2 – Viewing audit information for workflows that have been removed.
- IKB-49 – MyID signing and encryption keys.
- IKB-72 – Cancel Credential and Unlock PIN options require two security phrases.
- IKB-154 – One per credential group option not supported by VSCs.
- IKB-159 – Error when modifying an email template.
- IKB-174 – Mobile still assigned to user after warning.
- IKB-175 – Card activation may fail if the verified fingerprint does not exist on the card.

  Note: MyID will now verify the fingerprint of the cardholder against any that they have enrolled with MyID, in line with FIPS-201-2 requirements.
- IKB-176 – Unlock Credential workflow requires updates for some cards.

- IKB-184 – Cannot use a signature pad with self-service activation.
- IKB-188 – Canceling a mobile device that has failed issuance.
- IKB-197 – Limited unblock attempts.
- IKB-199 – Error when upgrading PIV installations.
- IKB-204 – Cannot cancel a bureau card awaiting activation.

5.7 End of life features

5.7.1 Physical signature option for Terms and Conditions.

You can no longer select the **Physically Sign** option for Terms and Conditions, which previously allowed you to use a signature capture pad to sign the terms and conditions.

If you are upgrading your system and have previously used this option, use the **Credential Profiles** workflow to update your credential profiles to use a different option.

5.7.2 Internet Explorer 9 and 10

Internet Explorer 9 and Internet Explorer 10 are no longer supported for MyID. MyID Desktop continues to require Internet Explorer 11 to display some workflows within the application.

For more information, contact customer support quoting reference SUP-258.

5.7.3 Windows 8

Windows 8 is no longer supported for MyID. Windows 8.1 continues to be supported, as do Windows 7 and Windows 10.

For more information, contact customer support quoting reference SUP-258.

5.7.4 Smart cards

The list of currently-supported smart cards and drivers in the ***Smart Card Integration Guide*** has been simplified.

If you are upgrading from an earlier version of MyID, and are using cards that are not listed in the ***Smart Card Integration Guide***, contact customer support quoting reference SUP-80.

If you are using older versions of minidrivers or middleware not listed in the ***Smart Card Integration Guide***, you are recommended to upgrade to the listed versions. For more information, contact customer support quoting reference SUP-80.

The following smart cards are no longer supported:

- Authenex v3.5
- Authenex v3.6
- Gemalto IDPrime .NET 510
- Gemalto IDClassic IAS 3610
- Gemalto IDClassic IAS 610
- HID Crescendo C700
- Keycorp GENO v4.10 / v 1.00
- Oberthur ID-One Cosmo v7.0n CosmopolIC Platform (with AuthentIC V3 Applet)

- Oberthur ID-One Cosmo v7.0n CosmopolIC Platform (with IAS-ECC Applet)
- Oberthur USB Slim v2 token (with AuthentIC V3 Applet)
- Oberthur USB Slim v2 token (with IAS-ECC Applet)
- Oberthur ID-One Cosmo v7.0.1-n Token Slim v2.0 (Authentic V3 Applet)
- Oberthur ID-One Cosmo v7.0.1-n Token Slim v2.1 (Authentic V3 Applet)
- Oberthur ID-One Cosmo v7.0.1-n Token Slim v2.0 (IAS-ECC Applet)
- Oberthur ID-One Cosmo v7.0.1-n Token Slim v2.1 (IAS-ECC Applet)
- RSA SID 600
- RSA SID 700
- RSA SID 800
- SafeNet SC650 V3
- Siemens CardOS 4.3B
- Siemens CardOS 4.4
- VASCO Digipass GO3
- VASCO Digipass 250
- VASCO Digipass 260

6 Previously in MyID 10.7 Update 1

6.1 Extended support for Elliptic Curve Cryptography

MyID 10.7 added the capability to issue certificates that use Elliptic Curve Cryptography (ECC) for key generation. This feature has been extended in this update release to allow ECC-based certificates to be used for MyID signing events, enabling:

- Logon to MyID with an ECC certificate.
- Collection of certificate updates and renewals to cards with ECC certificates.
- Using a PIV card with an ECC PIV-Auth certificate to authenticate to the MyID Derived Credential Self-Service Kiosk.

6.2 Support for Yubico YubiKey 4 devices

MyID now supports Yubico YubiKey 4 devices.

These are small USB-based devices that can be personalized to provide the same functionality as PIN-protected smart cards.

MyID can set a user PIN and provision certificates to the devices, enabling the use of certificates for authentication, email signing, and encryption.

See the ***Smart Card Integration Guide*** for details.

6.3 Updated support for SafeNet devices

MyID now supports SafeNet eToken 5110 devices and SafeNet Authentication Client version 10.1. See the ***Smart Card Integration Guide*** for details.

6.4 Support for Gemalto PIV cards using SCP03

MyID now supports Gemalto ID Prime v2.0 PIV cards with secure channel SCP-03 and AES-128 PIV 9B keys (Gemalto customer item C1072203).

See the ***Smart Card Integration Guide*** for details.

6.5 Support for SQL Server 2016

You can now install the MyID database tier on SQL Server 2016. This has been tested using SQL Server 2016 Cumulative Update 1 (version 13.0.2164.0).

Note:

- Microsoft SQL Server Full Text Search feature must be enabled.
- MyID does not support Database Mail with this version of SQL Server – you must use the SMTP Mail feature instead. See section *9.2*, *Enhanced email capability*.

6.6 Mobile enhancements

MyID Identity Agent now supports credential issuance to mobile devices with iOS 10.

6.7 Issued devices list in the System Status report

The **System Status** report generated by MyID now incorporates a summary of the number of issued devices for each device type. This allows Intercede to understand ongoing device support requirements for a customer installation.

6.8 Known issues resolved in MyID 10.7 Update 1

The following known issues have been resolved in the current version of MyID:

- IKB-180 – Zebra printers not supported with new Print Card workflow
- IKB-193 – Updates required for Gemalto IDPrime PIV cards
- IKB-200 – Some smart cards will not reset GlobalPlatform keys to factory values
- IKB-201 – Error when attempting to erase a partially-issued Intel VSC
- IKB-203 – Support for Oberthur PIV cards with Applet v2.3.5

6.9 End of life features

6.9.1 SQL Server 2012

Older versions of Microsoft SQL Server 2012 (RTM, SP1) are no longer supported for new installations of MyID. At minimum, SQL Server 2012 SP2 (version 11.0.5058.0) is required.

6.9.2 SafeNet smart cards

The following SafeNet smart cards are no longer supported in MyID.

- SafeNet iKey 2032 (however, the unblocking version SafeNet iKey 2032u is still supported)
- SafeNet Smartcard SC330
- SafeNet Smartcard SC330u
- SafeNet eToken 5000
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5200
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

7 Previously in MyID 10.7

7.1 Intel Virtual Smart Cards

Intel Identity Protection Technology is available in the 5th and 6th generation of Intel Processors with vPro technology, and provides a secure environment that can:

- Securely generate tamper resistant, persistent RSA key pairs in hardware.
- Generate PKI certificates from hardware protected RSA key pairs.
- Perform RSA private key operations within a protected hardware environment.
- Protect key usage using PINs that use the Intel IPT with PKI protected transaction display.

Using this technology, MyID can create a Virtual Smart Card that provides PIN protected access to certificates. The private keys of each certificate are protected within the Intel secure environment.

This enables two-factor authentication use cases such as:

- Windows Logon.
- Authentication to SSL protected web sites.

The user PIN is entered with the Intel Protected Transaction Display – a secure user interface generated from within the Intel environment. As this is not part of the Windows operating system, it is protected from malware and key loggers adding an additional layer of security.

Intel Virtual Smart Card support is available on compatible computers running Windows 8.1, or Windows 10.

If you want to use Intel Virtual Smart Cards on Windows 7 clients, contact Intercede customer support quoting reference SUP-245.

7.2 New workflows

This release of MyID includes new workflows within MyID Desktop. This continues the migration away from using embedded Internet Explorer-based workflows.

7.2.1 Erase Card

The **Erase Card** workflow replaces the old **Cancel Card** workflow, and allows you to unassign the card from the user, revoke and remove any certificates stored on it and return the card to as close to its original state as possible. You can erase smart cards that are physically present, and VSCs that are stored on the machine on which you are running MyID Desktop.

See the ***Administration Guide*** for details.

7.2.2 Cancel Credential

The **Cancel Credential** workflow replaces the old **Remote Cancel Card**, **Cancel ID**, **Request Cancel Card**, and **Confirm Cancel Card** workflows. It allows you to cancel a credential (mobile identity, smart card, virtual smart card) where the credential is not present. The device is unassigned from a person in the MyID database, and its certificates revoked. The device is not physically altered.

See the ***Administration Guide*** for details.

7.2.3 Reset Card PIN

The **Reset Card PIN** workflow replaces the old **Unlock Card** and **Change PIN** workflows. It allows you to change the PIN for a smart card or virtual smart card connected to MyID Desktop, or reset the PIN when it has been forgotten or the PIN has been locked. The workflow enforces authentication of the card holder – you can configure which authentication methods are available using the **Edit Roles** workflow; you can use:

- Identity documents
- Security questions
- The existing card PIN
- Authentication codes
- Operator approval

You can also configure MyID to allow you to reject the authentication, or to bypass the authentication altogether.

See the ***Administration Guide*** for details.

7.2.4 Unlock Credential

The **Unlock Credential** workflow replaces the **Remote Unlock** and **Unlock ID** workflows, and allows you to unlock a user PIN where the device is not connected to MyID using challenge/response unlocking. The user with the locked credential calls up the helpdesk, and the helpdesk operator then uses the **Unlock Credential** workflow to provide the unlock code.

This feature is supported with compatible smart cards, virtual smart cards, and mobile devices.

See the ***Administration Guide*** for details.

7.2.5 Print Card

The **Print Card** workflow replaces the old version of the **Print Card** workflow, and allows you to use a card printer to print the surface of an already-issued smart card that has a contact chip that allows it to be identified by MyID.

See the ***Administration Guide*** for details.

7.2.6 Upgrading systems to use new workflows

MyID 10.7 introduces the following workflows:

- **Erase Card** – replaces the old **Cancel Card** workflow.
- **Reset Card PIN** – replaces the old **Unlock Card** and **Change PIN** workflows.
- **Print Card** – replaces the old version of the **Print Card** workflow.
- **Cancel Credential** – replaces the **Remote Cancel Card**, **Cancel ID**, **Request Cancel Card**, and **Confirm Cancel Card** workflows.
- **Unlock Credential** – replaces **Remote Unlock** and **Unlock ID**.

To use these new workflows, you *must* use the latest MyID Desktop clients. If you do not upgrade MyID Desktop to the latest version, you will still be able to use the old versions of the workflows, but the new workflows will not appear in your list of available workflows.

You must use the **Edit Roles** workflow to provide permissions to the new workflows. You will then be able to use the new workflows; note, however, that you will no longer be able to see or use the old, replaced workflows.

For more information on upgrading to the new workflows, contact customer support quoting reference SUP-238.

Intercede understands that for large enterprises, deploying new clients can take time, and is therefore maintaining support for the old workflows (when used with the older versions of MyID Desktop or the web user interface) as described above.

This is intended to give customers time to update their clients, and customers should expect that over time support for the old workflows will be dropped.

7.2.7 Searching for people in the new workflows

The **Unlock Credential** and **Cancel Credential** workflows make use of a simplified but powerful search capability that allows one search box to match against first name, last name, full name, and logon name. It also allows a "fuzzy match" capability so that close matches are also returned in the results list.

See the *Entering search criteria* section of the ***Administration Guide*** for details of using this search feature.

This new search capability requires the Microsoft SQL Server Full Text Search feature; see the ***Installation and Configuration Guide*** for details. This feature is part of the SQL Server database engine, and is an option that you must enable on the installation of SQL Server. Configuration of the search feature, once enabled on the database platform, will be taken care of by the MyID installer at the time of installation.

7.3 Import and distribute certificates to devices

The MyID credential management system has advanced functionality for ensuring archived certificates are securely delivered to smart cards, virtual smart cards, and mobile devices, including recovery of historic certificates; for example, those used to encrypt emails.

This capability has now been enhanced to allow a user to import certificates that were not originally issued by MyID, into MyID, enabling MyID to take over the deployment and management of the certificates.

Based on the policy of the organization, the certificates can be recovered to a physical smart card, virtual smart card, or mobile device that supports key recovery capabilities.

An organization can also decide if a device is secure enough to store an archived certificate – for example, allowing recovery to the user's physical smart card but not to their mobile device with software key stores only.

Certificates are imported as PFX files – the **Upload PFX Certificates** workflow is used to upload one or more PFX files to the MyID server and associate them with a certificate policy.

For more information, see the *Import and distribute certificates to devices* section in the ***Administration Guide***.

7.4 Temporary Virtual Smart Cards

Many organizations use a physical smart card as the primary credential for each employee – it can provide a graphical ID badge, physical access control, and also strong two-factor authentication to computers and other electronic resources. Physical cards can be lost, forgotten, or damaged. When this occurs, users need to be able to gain access to resources as quickly as possible, in the most convenient way, to allow them to continue to work without reducing the security a smart card provides.

MyID can deploy virtual smart cards (VSCs) to a computer with a Trusted Platform Module (TPM), providing a secure alternative to the physical smart card. VSCs can be deployed in advance; for example, following a physical smart card logon to the computer, with the user PIN of the VSC created in a locked state, so it is not immediately usable.

When access to the VSC is required, the user can contact a helpdesk who will guide them through a PIN unlock process – this does not need network access so can take place away from the office. The helpdesk can also specify how long the user is able to use the VSC.

When the user's physical smart card is enabled (for example a replacement is issued, or the card itself is re-enabled) or expiry of use of the VSC is reached, MyID will lock the user PIN of the VSC when it is next connected to the network, in effect disabling the temporary credential.

This helps organizations enforce use of a smart card as a primary credential, while providing a simple and secure alternative should the primary smart card be unavailable.

Note: This feature is currently available for computers running Windows 7. If you want to use this feature with computers running a later Windows operating system, contact Intercede for further information.

For more information, see the *Unlocking VSC temporary access* section in the ***Microsoft Virtual Smart Card Integration Guide***.

7.5 Microsoft Azure

This release of MyID now supports a MyID server deployment into a Microsoft Azure environment. As part of this integration, MyID now supports the Microsoft Azure SQL Database platform.

Note: As Microsoft Azure is a cloud platform, network connectivity may differ from that of an on-site MyID deployment. The appropriate network connectivity must be in place for MyID to operate; it is recommended that particular attention be paid to third party connected systems such as PKI or IDMS solutions.

See the ***Microsoft Azure Integration Guide*** for further details.

7.6 Mobile enhancements

The MyID Identity Agent now supports credential issuance to mobile devices with Windows Phone 10.

7.7 Additional features

7.7.1 ECC support

MyID now supports issuance of certificates incorporating Elliptic Curve (ECC) keys. ECC provides higher levels of security with shorter key lengths when compared to RSA keys. This can provide faster key generation and key usage; for example, when signing or encrypting data.

This support is dependent on certificate authority and smart cards in use. If you want to make use of this feature, contact Intercede for further details quoting SUP-237.

7.7.2 Enhanced automatic key recovery at certificate renewal

When a certificate renewal is collected, MyID will also check for any archived certificates (for example, email encryption certificates) that should be recovered to the device.

The rules for which certificates to recover, and how many, are determined by the credential profile assigned to the device. Older certificates may be removed, depending on the profile configuration.

This feature is available for smart cards, Microsoft virtual smart cards, and mobile devices that support key recovery.

7.7.3 Bureau issuance

An additional module is available that supports bureau issuance of PIV cards using the Oberthur card personalization bureau.

For more information, or to discuss integration with other card personalization bureaus, contact customer support quoting reference SUP-233.

7.7.4 Fargo HDP 8500

MyID now supports the Fargo HDP 8500 smart card printer. This printer is a high volume industrial printer, ideally suited to card production facilities. MyID support chip personalization, card surface printing, and identification of PROX IDs with these printers, where compatible smart card readers are used.

For more information, see the ***Printer Integration Guide***.

7.7.5 Additional Identities API

The Credential Web Service module (CWS) has been enhanced to enable an additional identity to be added or removed from a MyID user account using an API call. An additional identity can represent another account belonging to the owner of the credentials; for example, a system administrator account used for accessing an alternative domain.

When the request is created by the API, an update job is created for the user's devices that can hold an additional identity – this is part of the credential profile configuration.

Collection of the job will add (or remove if appropriate) the additional identity from the device.

For more information, see the ***Credential Web Service*** document.

7.7.6 Assigning cards

You can use the **Assign Card** workflow to assign a particular smart card to a card request job. The user can then use only the specific card that has been assigned to that job in the **Collect Card** or **Collect My Card** workflows.

See the *Assigning cards* section in the in the ***Administration Guide*** for details.

7.7.7 Email PIN option

The **Email PIN** option in the **Credential Profiles** workflow is now located in the **PIN Settings** section, and is available only when the **Issue With** option is set to **Client Generated PIN** or **Server Generated PIN**.

7.7.8 Customizing terms and conditions

The way you provide customized terms and conditions has now been simplified. Instead of having to use the MyID translator tool to change the wording, you can now create a text file on the MyID web server that overrides the standard terms and conditions.

See the *Customizing terms and conditions* section in the ***Administration Guide*** for details.

7.7.9 Allow self requests option

The **Allow self requests** option on the **Self-Service** page of the **Security Settings** workflow now has a default of `No` for new installations. This means that, by default, operators cannot request a card for themselves using the **Request Card**, **Request Replacement Card**, **Issue Card**, **Request Card Update** or **Batch Request Card** workflows.

Note: To prevent upgrading systems from losing functionality, if you upgrade to the current version of MyID from a system that does not have this configuration option, the default value is set to `Yes`. If you upgrade from a system that *does* have this configuration option, the value is left unchanged.

7.7.10 Activation and unlock options for MyID Desktop

You must now provide the serial number and device type for the smart cards you want to activate or unlock when using the `/activate` and `/unlock` command-line options for MyID Desktop. Previously, the serial number and device type were optional.

7.7.11 Request External Certificates workflow

Prior to version 10, MyID provided the **Request External Certificates** workflow which enabled an externally generated PKCS#10 certificate request to be processed, and the certificate returned as a file for installation on a computer or server.

Currently, this workflow is not available as part of the base product installation – if you want to make use of it, contact Intercede customer support quoting reference SUP-244.

7.8 Technical enhancements

7.8.1 Document scanning

Use of EZTWAIN for scanning has been replaced with a simpler integration method. TWAIN scanning is no longer supported, and the standard WIA2 method is used instead.

You do not need to set the **Scanner driver support** configuration option.

If you are upgrading from an earlier version of MyID, and need to retain support for a TWAIN scanner, contact Intercede customer support for further guidance.

7.8.2 Enhancements to data model storage location

In earlier versions of MyID, data model files, which are used for device personalization, existed in multiple locations: within the website, the web services, and on the application server. If new data models were deployed, or modifications to data models were made, it was necessary to ensure that the changes were deployed to all locations. This created the possibility of the locations being out of synchronization, which could lead to inconsistent behavior in MyID.

The application server is now the repository for *all* data models, and by default any data models not on the application server are ignored.

If you have a MyID 10.7 installation with old Windows clients that are being used to activate PIV cards, these old clients may not be compatible with this change, causing device personalization to fail, with the following error being written to MyID system events:

```
Legacy datamodel configuration is disabled
```

If this occurs, you are recommended to update the old MyID clients. However, if this is not possible, you can re-enable the old data model processing behavior by setting the **Allow Legacy Data Models** option on the **Server** tab of the **Security Settings** workflow to `Yes`.

Once you have updated all your old clients, set the option back to `No`.

7.8.3 Web service user

This version of MyID introduces the MyID web service user as a third MyID user account.

Previous versions of MyID ran the web services as the MyID COM+ user. Introducing the web service user, which is dedicated to running the web services, enables unnecessary privileges to be removed from the web service, thus improving security.

When you install this version of MyID, you must specify the MyID web service user. This account must have the same permissions as the MyID IIS user.

If you are upgrading from a previous version of MyID, you must create this account before you install the current version of MyID.

For details, see the ***Installation and Configuration Guide***.

7.8.4 COM+ encryption

In previous versions of MyID, when each MyID COM+ component was installed, the DCOM Security **Authentication Level for Calls** option was set to the default level **Packet**. The ***Installation and Configuration Guide*** provided information on setting this option to **Packet Privacy** for an extra level of security in server to server communications (for example, where the web server needed to be more accessible) – however, this setting reverted to the default whenever you installed MyID or installed a patch that modified the MyID COM+ components.

From this version of MyID, to ensure security, the **Authentication Level for Calls** option is set to **Packet Privacy** by default.

For more information, contact customer support quoting reference SUP-232.

7.8.5 Editing Certificate Authority details

You can now update a wider range of settings for certificate authorities registered in MyID. This allows updates, for example, to stored passwords or connectivity files.

For further details, see the certificate authority integration guides.

7.8.6 Storing HSM PINs

GenMaster now stores the PINs for SafeNet HSMs as encrypted values in the registry for the MyID COM+ user. This allows automatic restart of the server to connect to the HSM without the user manually entering the PIN.

If you are upgrading an existing SafeNet HSM system and want to migrate the PIN, or if you are using a Thales nShield HSM and want to store the PIN, or if you want to change the stored PIN for an HSM, you can use the SetHSMPIN utility to do this.

For details, see the ***Installation and Configuration Guide***.

7.8.7 Stored procedure for sending SMS

Before MyID 10.7, the stored procedure that sent SMS messages for mobile notifications was called `sp_CustomSendSMS`; from MyID 10.7, this stored procedure is called `sp_CustomPrepareSMS`.

If you have made any customizations to your `sp_CustomSendSMS` stored procedure, you must review the content of the `sp_CustomPrepareSMS` stored procedure to ensure that it meets your requirements.

7.9 End of life features

These features are no longer available for new installations of MyID. There is limited support for upgrading customers – please contact Intercede for further details.

7.9.1 Replaced web operations

See section *7.2.6*, *Upgrading systems to use new workflows* for details of configuring your system to use the replacements for these workflows.

- Cancel Card
- Remote Cancel Card
- Cancel ID
- Request Cancel Card
- Confirm Cancel Card
- Unlock Card
- Change PIN
- Remote Unlock
- Unlock ID
- Print Card (web version)

7.9.2 Support for TWAIN drivers when scanning documents

Previously, MyID required TWAIN drivers and third-party integration software to support document scanning. This requirement has now been replaced with support for WIA2 drivers.

7.9.3 Server-generated Virtual Smart Card

Microsoft Virtual Smart Cards can be issued using a server-generated process (requiring the client computer to be a member of the same domain as the MyID server), or created using a client-generated process which does not have the same restriction. The client-generated VSC feature was introduced in MyID 10.4. The server-generated VSC feature is no longer available on new installations of MyID. If you are upgrading from an earlier version of MyID, and are using server-generated VSCs, MyID will continue to support lifecycle management of the issued VSCs. You can continue to issue new server-generated VSCs; however, note that some additional software and configuration is required. You can also migrate from issuing server-generated VSCs to client-generated VSCs.

For more information, contact customer support quoting reference SUP-246.

The ***Microsoft Virtual Smart Card Integration Guide*** supplied with this release contains instructions for setting up MyID to issue VSCs using the client-generated process.

7.10 Known Issues resolved in MyID 10.7

The following known issues have been resolved in the current version of MyID:

- IKB-53 – Upgrading can undo environment configuration

- IKB-55 – Certificates not written to reinstated card with 1-step pre-encode
- IKB-56 – Uncollected certificates not revoked
- IKB-57 – Some OEM versions of Lollipop block provisioning link in email
- IKB-64 – Tapping a renewal notification link
- IKB-70 – Configuring the request validation mode
- IKB-73 – Known mobiles option not supported
- IKB-75 – Limitation of whenChanged
- IKB-77 – User uploaded PFX files cannot be issued to mobile
- IKB-78 – TokenImport.exe file installed to wrong location
- IKB-85 – Issue selecting credential profiles
- IKB-90 – misleading error message when certificate policies are disabled
- IKB-91 – Historic encryption certificates are not removed from the mobile device during update
- IKB-93 – Failing NIST tests
- IKB-96 – Error collecting archived certificate renewal
- IKB-97 – Mobile logs do not always display
- IKB-98 – Updates do not remove old archived certificates
- IKB-99 – VSCs not re-enabled automatically when temporary replacements are cancelled
- IKB-101 – Remove Person does not revoke certificates
- IKB-109 – Cannot log on to MyID with a certificate key length set to Default
- IKB-119 – Challenge code requests require a user account
- IKB-120 – Apply Update notification is sent at the end of the 2-step pre-encode process
- IKB-123 – Identity Agent does not support SHA-256 passwords
- IKB-125 – Cannot log on to Windows 8.1 or Windows 10 with Oberthur ID-One PIV (v2.3.5) cards
- IKB-136 – Kiosk stops responding if Federal Bridge check fails
- IKB-138 – Uninstall may not remove all components
- IKB-142 – Key name issue
- IKB-143 – Problems using two-way SSL for MyID Desktop
- IKB-144 – Expiry dates on replacement cards
- IKB-145 – Incorrect setting for PIV key history containers
- IKB-146 – Security phrases required when credential profile does not specify them
- IKB-151 – Copying credential profiles does not copy all settings
- IKB-156 – Certificate Server does not automatically restart on connection failure
- IKB-158 – The list of credential profiles in Validate Request includes profiles that are not supported for Intel Virtual Smart Card

8 Previously in MyID 10.6 Update 1

8.1 Configurable number of security questions for authentication

You can configure MyID to request a random selection of security questions for authentication; for example, you may require your users to have six security phrases registered, and configure MyID to ask two of those questions when authenticating.

Also, the **Number of security phrases** option has been renamed **Number of security questions to register**.

For more information, see the *Setting the number of security phrases required to authenticate* section in the ***Administration Guide***.

8.2 Configuring authentication for unlocking

Previous versions of MyID used the following configuration options to configure the authentication used for unlocking:

- **Remote Unlock requires Security Phrase prompt**
- **Remote Unlock requires an Authentication Code prompt**

These options are no longer supported, and have been replaced by role-based permissions that provide you with much greater flexibility in determining which users can use these features.

For more information, see the *Unlocking a card remotely* section in the ***Administration Guide***.

8.2.1 Upgrading existing systems

If you upgrade an existing system:

- If the **Remote Unlock requires Security Phrase prompt** configuration option is set to `Yes`, the upgrade process will add the **Security Questions** sub-option to every role that has access to the main **Remote Unlock** workflow.
- If the **Remote Unlock requires an Authentication Code prompt** configuration option is set to `Yes`, the upgrade process will add the **Authentication Code** sub-option to every role that has access to the main **Remote Unlock** workflow.

8.3 Configuring authentication for mobile unlocking

Note: From MyID 10.7, the **Unlock ID** workflow has been superseded by the **Unlock Credential** workflow.

Mobile identity users may need to contact their helpdesk to unlock their devices. The helpdesk operator can use the **Unlock ID** workflow to provide a code that unlocks the mobile.

To set up authentication methods for mobile unlocking:

1. From the **Configuration** category, select **Edit Roles**.
2. In the **Mobile** section, set the following sub-options for **Unlock ID**:

- **Operator Approval** – if the mobile user cannot provide alternative authentication, the operator can override the check. The operator *must* provide a reason why they are providing approval.
- **Security Questions** – the mobile user can unlock their device by providing the answers to their security questions.

  The number of security questions the user must answer is determined by the **Number of security questions for operator authentication** option. See the *Setting the number of security phrases required to authenticate* section in the ***Administration Guide***.

Assign these options to the appropriate roles; for example, you may want users who have one role to use security questions, and users who have another role to require operator approval.

Note: You must select at least one method of authentication. The user will not be able to unlock their device unless they can authenticate using one of these methods.

3. Click **Save Changes**.

For information on using the **Unlock ID** workflow, see the ***Mobile Identity Management Installation and Configuration Guide***.

8.4 LDAP update

During credential lifecycle events (such as issuance or revocation), MyID can send updates to a connected directory. This can be used to set specific attributes against a user; for example, setting or removing the requirement to log on to Windows using a smart card.

This feature requires careful configuration. For more information, contact customer support, quoting reference SUP-227.

8.5 Launching MyID Desktop with automatic Windows Logon

You can configure MyID Desktop to attempt to log on using Integrated Windows Logon when it starts up, instead of having to select the option on the logon screen:

```
MyIDDesktop.exe /lw
```

See the ***Administration Guide*** for details of setting up your system to allow Integrated Windows Logon.

8.6 Unlock My Security Phrases workflow

You can allow users to unlock their own security phrases by giving their role access to the **Unlock My Security Phrases** workflow. The user can authenticate to MyID with some other method (for example, smart card or logon code) then use this workflow to unlock their security phrases without any further authentication.

See the ***Administration Guide*** for details.

8.7 Wildcard serial number search in Request Card

The new configuration option **Allow card serial number to be entered during Request Card workflow** (on the **Devices** tab of the **Operation Settings** workflow) allows you to specify a serial number when using the **Assign Card** feature in the **Request Card** workflow.

You can use `?` and `*` as wildcard characters in this search. Any unassigned devices, or devices with unrestricted cancelation, that match the search criteria are displayed. The limit is 10 records; if more than 10 devices match the search criteria, you must search again with more restrictive criteria.

See the ***Administration Guide*** for details.

8.8 Controlling the visibility of device history tabs

You can control whether the device history tabs are visible in the **Identify Card** and **View Person** workflows:

- In the **Identify Card** workflow, the **Card History** tab appears only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.
- In the **View Person** workflow, the **Credentials** and **History** tabs appear only if your role includes the **View Device Details** option in the **Cards** section of the **Edit Roles** workflow.

See the ***Administration Guide*** for details.

8.9 Unrestricted cancelation

The **Unrestricted Cancelation** option in the **Issuance Settings** section of the **Credential Profiles** workflow controls whether you can re-use a card without first cancelling it. Even if the card has already been issued, this allows you to issue the card or assign it to a request; the previous credentials will automatically be cancelled with a status mapping of Lost, and a comment indicating that the card was cancelled by the unrestricted cancelation feature.

This option appears only if the **Enable unrestricted cancelation** option on the **Issuance Processes** tab of the **Operation Settings** workflow is set to `Yes`.

You may find this feature useful when setting up a credential profile for temporary smart cards – you can maintain a stock of cards that can be used for temporary credentials and reuse them quickly without having to go through the cancelation process.

See the ***Administration Guide*** for details.

9 Previously in MyID 10.6

9.1 Updated user interface

MyID Desktop has an updated user interface for version 10.6, providing a more modern look and feel to enhance the user experience. In this release, the features updated include:

- Log-on processes.
- New ways of navigating categories and starting workflows.
- A dashboard of recently-used workflows.
- Rebranded web-based workflows.
- Enhanced confirmation screens.

See *The interface* section in the ***Administration Guide*** for details.

9.2 Enhanced email capability

MyID provides a new system for sending email messages that removes the dependency on SQL Server. Instead of sending messages through Database Mail within SQL Server, you can now specify an SMTP server using the **External Systems** workflow. You can configure this SMTP server to use SSL/TLS for security.

This enables you to use an enhanced notifications mechanism, providing the ability to search and review the status of notifications sent by MyID, and resend them when the associated jobs are still active.

You can also set up multiple SMTP servers – MyID will send email notifications to each configured external system.

For more information, see the *Setting Up Email* section in the ***Installation and Configuration Guide***.

If you are upgrading an existing system, your Database Mail configuration will continue to work. If you want to switch to the new system, carry out the following:

1. Set up a new SMTP server in the **External Systems** workflow.
2. Set the **Database Mail Profile Name** option to empty.

9.3 Signed email notifications

You can now configure MyID to send email notifications as cryptographically-signed messages. This provides additional visible levels of trust for end users when they receive the notification.

Note: This feature is not available if you continue to use Database Mail for your email notifications.

For more information, see the *Signing email messages* section in the ***Installation and Configuration Guide***.

9.4 Mobile identities

Mobile Identity Management support is built into MyID 10.6. Previous versions of Mobile Identity Management required the installation of a separate module.

Support for Derived Credentials is now provided by a separate module. For more information, contact customer support, quoting reference SUP-217.

9.5 Enhanced HSM Test Utility

A utility is provided with this release to help confirm configuration with Hardware Security Modules (HSMs). This tool mimics the PKCS#11 transactions used by MyID and will exercise all functions of the HSM that MyID requires. You can use this utility to test cryptographic performance on the system; for example, to determine the optimum number of threads (concurrent operations) to achieve the best scalability for a given HSM.

You can find this utility in the `HSM Integration\HSM Test Utility` folder on the MyID product CD.

9.6 Client Components version options

The following options are not supported in MyID Desktop:

- **Minimum Supported Client Components Upgrade Action**
- **Minimum Supported Client Components Version**
- **Preferred Client Components Version**
- **Preferred Client Components Version Upgrade Action**

For more information, contact customer support, quoting reference SUP-219.

9.7 Database names in email messages

Previous versions of MyID provided email templates that included a substitution value for the name of the database sending the email message. As MyID no longer uses Database Mail to send email messages, this is no longer possible.

Email templates that included messages similar to the following have been updated:

```
Database %1 is approaching its credential licence limit.
```

If you have made any changes to these email templates, these will have been overwritten when you installed MyID 10.6. You must review your templates to ensure that they are correct.

9.8 Logon Name Required option

The **Logon Name Required** option (on the Logon page of the Security Settings workflow) is no longer supported. The option will appear only on systems that have been upgraded from older versions of MyID, but will not have any effect on MyID's behavior.

9.9 Mobile identity management changes

Release 10.6 contained the following mobile identity management changes:

- Support for issuing certificates to separate keychains on an iOS device.

  Certificates can now be written to separate keychains in a single collection process. For example, a Wi-Fi authentication certificate can be held in the device's native key store, while email signing and encryption certificates can be stored in a PIN protected keychain for additional security. This capability is fully configurable allowing flexibility to meet the security policies of your organization.

  Note: Issuing a mobile identity with certificates in multiple key stores will consume a MyID credential license for each key store.

- Fingerprint support in MyID Mobile SDK – iOS.

  App developers can now enable fingerprint protection for certificates using the MyID Mobile SDK for iOS. This provides greater convenience for end users as an alternative to using a PIN to authenticate themselves for signing/encryption operations.

- Support for Android 6 (Marshmallow).

  The Identity Agent and Mobile SDK are now supported on the latest version of Android's operating system.

- Deleting credentials from mobile devices

  You can now delete credentials directly from the mobile device, removing certificates and associated credential data from the device. Note that this does not update the MyID server, which means that issued certificates will remain active.

- Improvements to URL handling in emails

  The mechanism for launching the MyID Identity Agent from a link in an email has been improved. The link is now encoded as an HTTP(S) URL, and will redirect to a web site that will launch the identity agent on the mobile device.

- Mobile Identity Management support is built into MyID 10.6.

  Previous versions of Mobile Identity Management required the installation of a separate module.

- Support for Derived Credentials is now provided by a separate module.

  For more information, contact customer support, quoting reference SUP-217.

- MIM-based credential profiles are no longer supported from MyID 10.6.

  Existing mobile identities that were issued using MIM-based credential profiles will continue to work; you can still renew certificates and apply updates. However, you cannot select MIM-based credential profiles within any MyID workflow, and you will see an error if you attempt to request an MIM-based credential profile using the Credential API. If you want to replace an MIM-based identity, you must select an Identity Agent-based profile for the replacement device.

- Numeric-only PINs are enforced

  When you select an Identity Agent-based credential profile, the profile is automatically configured to require numeric-only PINs. Previously, you had to configure the credential profile manually.

10 Previously in MyID 10.5

10.1 Automated certificate updates across devices

Many employees now access IT services from a range of different devices – computers, smart phones and tablets. Certificates can be used on each device to establish trust in both the device and the user. On occasion, the keys and certificates need to be shared across devices to allow more than one device to carry out a particular task – for example, decrypting emails.

However, controlling the process for the issuance and lifecycle management of certificates across multiple devices can be complex and technically challenging. MyID now makes it easy.

For each managed certificate policy, MyID can now control how certificates are shared between devices – for example, enabling certificates to be shared on devices with a built-in security chip, but not on lower security devices such as a phones with software-based key stores.

Certificates that have been revoked and replaced can automatically be replaced on each device, meaning that the older certificates can still be used for the decryption of historical encrypted data. In addition, when a new certificate is needed – for example, if a device has been lost or stolen, an update can be automatically generated for each device that has the certificate.

Combined with MyID's self-service collection features, this enables you to simplify the management of devices throughout your organization and lower the cost of updating each device manually.

10.2 Certificate configuration updates

10.2.1 Selecting certificates in credential profiles

The Select Certificates stage in the **Credential Profiles** workflow has been significantly updated to incorporate options for certificate recovery.

See the ***Administration Guide*** for details.

10.2.2 Certificate configuration options

The following certificate configuration options have been removed:

- **Historic certificates to issue to a permanent replacement card**
- **Maximum number of certificates to automatically recover to a card at reprovision**
- **Historic certificates to issue to a temporary replacement card**
- **Global Historic Certificates**
- **Recover certificates for replacement cards**
- **Recover revoked certificates during card replacement**
- **Reprovision card recover any certificates**
- **Permanent replacement card recover any certificates**
- **Temporary replacement card recover any certificates**

The behavior determined by these configuration options has been replaced by the new Select Certificates stage in the **Credential Profiles** workflow.

When you upgrade your system from an earlier version of MyID, the upgrade script will update your credential profiles to match the behavior of your system as closely as possible. For more information, contact customer support, quoting reference SUP-202.

10.3 Enhanced credential updates

Processing updates to issued credentials has been enhanced in this release – when collecting an update to issued credentials, the content of the latest version of the assigned credential profile is checked, and any new certificates assigned to that profile are issued, or recovered depending on the credential profile configuration. Additional Identities are also checked, with new certificates issued where needed and older certificates removed when no longer associated with the device owner.

Updates can also be generated for devices belonging to the user hold a shared certificate when requesting a replacement device, using the new **Compromised – Reissue Shared Certificates** reason. See the *Certificate reasons* section of the ***Administration Guide*** for details.

10.4 Support for Windows 10

MyID administration and self-service user interfaces are now supported on Windows 10, including issuance and lifecycle management of Microsoft Virtual Smart Cards and physical smart cards with a PIV or compatible Windows minidriver interface.

See the ***Installation and Configuration Guide*** for details of supported operating systems.

10.5 Enhanced PIN policy rules

This release allows you to limit the number of repeated or sequential characters in a user's PIN.

See the section on setting the PIN Settings in the *Managing Credential Profiles* chapter of the ***Administration Guide*** for details.

10.6 Microsoft Virtual Smart Card (VSC) improvements

Requests for VSCs can now be targeted at a named computer when made through the MyID Credential Web Service API, limiting the collection of the request to a named user account on a specific computer.

See the `RequestCredentialForDevice` method in the ***Credential Web Service*** document.

This release also includes a new integration guide, providing further information on deploying VSCs and a utility to check the status of the TPM.

See the ***Microsoft Virtual Smart Card Integration Guide***.

10.7 Additional updates

Additional updates have also been made to support the following:

- Gemalto SafeNet Luna SA Hardware Security Module running 6.22.0 firmware using the v6.0 version of the Luna client software.
- Gemalto SafeNet Authentication Client v9.0.43 smart card software.
- Giesecke & Devrient SmartCafé Expert 6.0 smart cards.
- Gemalto IDPrime smart card Windows minidriver v8.4.8.0.

10.8 Email credential PIN at issuance

The following configuration option has been removed:

- **Email credential PIN at issuance**

Whether a PIN is sent in an email message to the cardholder at issuance is now controlled entirely by the **Email PIN** option in the credential profile.

See the ***Administration Guide*** for details.

11 Previously in MyID 10.4

11.1 Enhancements to Microsoft Virtual Smart Card support

MyID can now issue and manage Microsoft Virtual Smart Cards (VSCs) for computers with a Trusted Platform Module that are not connected to the same domain as the MyID server. This means that users across disparate networks, or even those connecting to MyID over the internet, can receive VSCs on devices running Windows 7 or Windows 8.1, allowing strong two-factor authentication to be used.

Server based generation and management of VSCs continues to be supported, with the addition of support on Windows 7. For more information, see the ***Administration Guide***.

11.2 Additional identities

MyID can now issue credentials for additional Windows accounts to the same smart card, making it easier to manage multiple user identities. This reduces the need for one person to have multiple smart cards to allow access to accounts used to provide higher levels of permissions or access to additional environments.

Using a direct connection from MyID to Microsoft Active Directory, additional user accounts can be retrieved and stored alongside the main MyID user account. A custom filter can be applied to ensure that the available user accounts meet your organization's naming convention for additional accounts. The certificate policy required can be selected from those available for additional identity certificates.

This is also available as a self-service operation – taking the workload away from system administrators. A more restrictive search policy can be applied to ensure only appropriate accounts can be selected for use. When the user is issued a smart card, the additional identity certificates are created and stored alongside the main certificates on the smart card. Each Windows logon certificate present on the card will be displayed on the windows logon screen when it is inserted to a card reader. Additional identity certificates can also be used for email signing, encryption, or VPN authentication. Further additional identities can be added to the user account, or removed causing revocation of the additional identity certificate. Re-issuing the card can create further additional identities certificates or remove previous certificates that are no longer required.

This feature is not currently supported for mobile devices or PIV cards.

See the ***Administration Guide*** for details.

11.3 Windows Integrated Logon

You can now use Windows Integrated Logon with MyID Desktop.

For more information on setting up Windows Integrated Logon, see the ***Administration Guide*** and the ***Web Service Architecture Installation and Configuration*** document.

11.4 Control which roles can validate credential requests

MyID now allows you to define which MyID roles can approve or reject credential requests, enabling better control over credential issuance processes. For example, it is now possible to ensure that requests for high security credentials can be approved only by MyID operators holding the role with authority to do so.

If you have the **Constrain Credential Profile Validator** option set, on the Select Roles page of the **Credential Profiles** workflow you can now select which roles can *validate* credentials using this credential profile. Select the roles in the **Can Validate** column.

To set the option, in the **Configuration** category, select the **Security Settings** workflow and click the **Process** tab.

11.5 HSM concurrency support

MyID now supports executing multiple KeyServer operations concurrently. This allows MyID to open several sessions on the HSM, improving the performance of transactions between the HSM and MyID.

By default, MyID creates up to ten concurrent sessions.

See the ***Installation and Configuration Guide*** for details.

11.6 AES256 master keys

When performing a new installation of MyID, the database master key will be generated as an AES256 key, providing stronger encryption for sensitive data. This is supported for software keys, or keys stored on either an nCipher HSM or a SafeNet HSM.

If you upgrade an existing installation of MyID to MyID 10.4 or later, the system will continue to use its existing database master key that was generated previously. If you require a pre-existing database master key to be changed to an AES256 master key, contact customer support for further information, quoting reference SUP-193.

11.7 VSC priority when collecting jobs in the Self-Service App

If the user is collecting a job that supports both contact and virtual smart cards (VSCs), the Self-Service App gives preference to the collection of a VSC over a contact card.

This is a change from previous versions, where the contact card would have been selected.

See the ***Self-Service App Installation and Configuration*** document for details.

11.8 End of life features

11.8.1 Removal of Abort On Failure? option

The **Abort On Failure?** option (on the **Certificates** page of the **Operation Settings** workflow) previously allowed the following options:

- **Always abort** – If a certificate fails to issue, MyID tells you what happened and gives you a link to abort the workflow.
- **Ignore error** – If a certificate fails to issue, MyID carries on and ignores the error, giving you no options.
- **Prompt user for action** – If a certificate fails to issue, MyID tells you what happened, and gives you two options, allowing you to abort or ignore the error.
- **Always abort but silently** – If a certificate fails to issue, MyID fails silently without any indication on-screen.

As ignoring errors results in cards issued with incomplete sets of credentials, this option has been removed from MyID, and the behavior is set to **Always abort**.

12 Previously in MyID 10.3

This section describes the changes that were made for the MyID 10.3 release.

12.1 Enhanced security features

This release of MyID introduces additional features to limit the information being returned to clients before authentication; this provides additional security by preventing potential attackers from gleaning feedback from unsuccessful attempts.

The messages that appear when a user fails to log on no longer provide the reason for the authentication failure, which would have allowed them to take corrective action; this may result in more calls to your helpdesk from users unable to authenticate to the system. You can still obtain details of the authentication failure from the **Audit Reporting** workflow. For some authentication operations, you may also want to check the information in the **System Events** workflow.

12.2 Simple Certificate Enrollment Protocol (SCEP)

MyID supports issuing device identities using the Simple Certificate Enrollment Protocol (SCEP). The MyID SCEP module enables customers to issue certificates securely to network devices, such as routers and firewalls, to improve security by protecting network traffic. This solution was designed to allow the issuance of certificates to devices in a scalable manner for large deployments including policy-driven control mechanism, validation process for authorized devices, and lifecycle management capabilities for the issued certificates.

The MyID SCEP module is provided as a separate software update.

See the ***SCEP Device Identities Integration Guide*** for details.

12.3 Simplified self-service smart card issuance

A number of features have been added to provide a more streamlined self-service collection process for smart cards and virtual smart cards.

12.3.1 Logon codes

As an alternative to pre-registering security questions in MyID, a logon code can be generated automatically and sent to the cardholder to allow access to MyID for collecting the credentials.

This option is available as part of a credential profile, allowing different policies to be set up for each credential type. This feature supports requests generated either by an external system (using the MyID Lifecycle API) or by an operator using the MyID user interface. The email template can be modified to suit your organizations requirements using the **Email Templates** workflow.

See the *Logon codes* section of the ***Administration Guide*** for details.

12.3.2 Launching new clients using a hyperlink or command line

Additional flexibility has been added to the startup process of MyID Desktop and the Self-Service Application. Both clients can now be started up either from a hyperlink or the command line, with the ability to access an operation directly, or launch a specific job (for example, a high priority card update). You can also embed hyperlinks within an email template, enabling a streamlined collection process when combined with a logon code.

See the following:

- The *Using logon codes* section in the ***Administration Guide*** for details of launching MyID Desktop with a hyperlink to use a logon code.
- The *Launching MyID Desktop* section in the ***Installation and Configuration Guide*** for details of launching MyID Desktop from a command line or hyperlink for logon codes, activation, or unlocking.
- The *Running the Self-Service App* section of the ***Self-Service Installation and Configuration*** document for details of launching the Self-Service App from a command line or hyperlink for a specific job.

12.4 Improved Batch Directory Synchronization Tool

The Batch Directory Synchronization Tool now checks for records that have been updated in the directory since the last run time, and only synchronizes this subset of records. This results in a much faster synchronization cycle over large scale directory deployments.

See the *Batch Directory Synchronization Tool* section of the ***Administration Guide*** for details.

12.5 Default roles and inheriting roles

You can set default roles for each group. These roles are automatically assigned to any new account added to the group. The default roles can also be inherited by any subgroups that are created within the group.

Note: This feature is not compatible with role assignment set at synchronization with the directory.

See the *Default roles* section of the ***Administration Guide*** for details.

MyID also allows you to specify whether the available roles for a group are inherited by their child groups. With role inheritance, if you change the roles available to the parent group, these roles are filtered down to the child groups.

See the *Role inheritance* section of the ***Administration Guide*** for details.

12.6 Restricting data returned in a Management Information Report

MyID now restricts the data retrieved from a Management Information Report to the data set that can be accessed by the current MyID operator based on their scope.

Note: This change is applied only to reports that contain a group field as part of their definition.

See the *Management Information (MI) Reports* section of the ***Administration Guide*** for details.

12.7 Certificate management for TPM based devices

The device identity issuance process has been improved to ensure that only one TPM-based device identity certificate will exist on the computer. When an existing certificate is re-issued, the previous certificate is now removed.

See the *Managing Devices* section of the ***Administration Guide*** for details.

12.8 Enhanced support for Entrust Certificate Authority

MyID can now integrate with Entrust Certificate Authority from Windows Server 2012, enabling support for Entrust across MyID Enterprise and MyID PIV. Changes to Distinguished Names in MyID can also be updated within Entrust.

See the ***Entrust CA Integration Guide*** for details.

12.9 Support for Thales nCipher PCI HSM

PCI form factor HSMs offer a cost effective alternative to network HSMs, so may be more suited to smaller deployments. MyID supports the nShield Solo range of PCI HSMs – all variants of this range are supported.

See the ***nCipher HSM Integration Guide*** for details.

12.10 eDB Data Import Server

The eDB Data Import Server is now deprecated, and the service will no longer be installed by the MyID product installation program. Previously, you had to disable this service to make use of the Lifecycle API – this is no longer required.

13 Previously in MyID 10.2

This section describes the changes that were made for the MyID 10.2 release.

13.1 MyID Desktop

MyID Desktop is the new user interface for MyID, and was introduced at MyID version 10.1. Instead of accessing MyID through Internet Explorer, MyID Desktop provides a Windows application that you can deploy to your end users.

Currently, MyID Desktop embeds parts of the MyID website, so for the time being you must set up the security options for Internet Explorer in the same way as for previous versions of MyID.

See the ***Installation and Configuration Guide*** for details.

Note: If you attempt to access MyID through Internet Explorer, you will see the following message:

```
This page is no longer available. Please contact your MyID administrator
for further information.
```

If you are upgrading from an earlier version of MyID that uses Internet Explorer as the primary user interface, contact Intercede customer support to discuss how to migrate to the new user interface, quoting reference SUP-160.

13.2 Licensing changes

MyID now provides increased flexibility in its licensing. In addition to user-based licensing, you can now track licenses for credentials issued – that is, smart cards, device identities, mobile identities, soft certificate packages, and so on.

For details of how the licensing system works, see the ***Administration Guide***.

13.3 Increased security for security phrases

MyID now uses SHA256 to store the answers stored for security phrases, providing significantly enhanced security. This feature is enabled by default for new installations.

If you are upgrading an existing system, see the ***Installation and Configuration Guide*** for details of migrating all your clients to use the new system.

13.4 Support for derived credentials

This release of MyID provides enhanced support for derived credentials on PIV systems. You can now issue mobile credentials that have been derived from smart cards that were issued by systems other than the current MyID system.

Mobile identities require an additional software package.

See the ***Derived Credentials Installation and Configuration Guide*** in the MyID Mobile Identity Management release for details.

13.5 Associating LDAP groups with MyID roles

You can now set up roles in MyID that are linked to groups in your LDAP. If you link the role to a group in the LDAP, any users in the directory that belong to that group automatically get assigned the corresponding role in MyID.

See the *Linking roles to LDAP* section in the ***Administration Guide*** for details.

13.6 Tracking users when their OU is changed in the LDAP

When you set the **Automatically create MyID groups from the Organizational Unit of imported users** option, and change the OU of a user in the LDAP, the user is moved to the appropriate group in MyID, creating the group if necessary. If you set this option to No, then move a user in the LDAP to an OU that does not have a corresponding MyID group, MyID displays a warning that the directory and the MyID database are no longer synchronized when you view the user's details in MyID.

13.7 Active Directory Deletion Tool

The Active Directory Deletion Tool allows you to synchronize Active Directory deletions.

See the *Active Directory Deletion Tool* section in the ***Administration Guide*** for details.

13.8 Specifying a certificate store in Microsoft CAs

You can now specify the certificate store to be used for EA certificates in Microsoft Certificate Authorities. Use the **Set Certificate Store** option in the **Certificate Authorities** workflow.

See the ***Microsoft Windows CA Integration Guide*** for details.

13.9 Increased length of email templates

You can now create email templates that are up to 8000 characters long.

See the ***Administration Guide*** for details of creating email templates.

13.10 Recovering archived certificates

You can now use the following configuration options to determine whether historic archived certificates that were previously issued to a user can be recovered to reprovisioned, temporary replacement, or permanent replacement cards, even if the card being reprovisioned or replaced did not hold the certificates:

- **Permanent replacement card recover any certificates**

  Whether archived certificates belonging to a user, but not to the card being replaced, are recovered onto a permanent replacement card.

- **Reprovision card recover any certificates**

  Whether archived certificates belonging to a user, but not to the card being reprovisioned, are recovered onto a reprovisioned card.

- **Temporary replacement card recover any certificates**

  Whether archived certificates belonging to a user, but not to the card being replaced, are recovered onto a temporary replacement card.

13.11 Reporting API web service

The Reporting API web service is not currently provided with MyID, as the MI Reports feature is no longer dependent on it. For more information about this web service and its inclusion in future releases of MyID, contact customer support, quoting reference SUP-159.

14 Previously in MyID 10.1

This section describes the changes that were made for the MyID 10.1 release.

14.1 MyID Desktop

MyID Desktop is the new user interface for MyID. Instead of accessing MyID through Internet Explorer, MyID Desktop provides a Windows application that you can deploy to your end users.

Currently, MyID Desktop embeds parts of the MyID website, so for the time being you must set up the security options for Internet Explorer in the same way as for previous versions of MyID.

See the ***Installation and Configuration Guide*** for details.

14.2 Support for SQL Server 2014

This release provides support for using Microsoft SQL Server 2014 as the MyID database.

See the ***Installation and Configuration Guide*** for details.

14.3 Key Recovery

You can now request and collect recovered keys onto the card of a different user from the original cardholder using a multi-stage process that includes:

- Creation of a key recovery request:
  - Retrieval of certificate owner information from a user account archive, in addition to the live MyID user account records.
  - Selection of the user account to collect the key recovery.
  - Certificate search based on a date range or a specified number of the most-recently issued certificates.
  - Specify an email address to receive details of the recovery card PIN.
  - Policy based approval stage of the request.
- Restricted collection of a request by a named user account.
- Generation of a randomized card PIN, with notification of the PIN to a named email account.
- Administrator operation to collect any key recovery request.

See the ***Administration Guide*** for details.

14.4 Device Identities

In MyID 10.0, lifecycle management of device identities was available using the Device Management API. In this release, you can also use MyID Desktop to request, validate, and cancel device identities.

See the ***Administration Guide*** for details.

14.5 Updated HSM support

MyID now supports the following:

- Luna SA HSM client software version 5.4.2.
- nCipher HSM client software version 11.70.

For more information, see your HSM integration guide.

14.6 Unlock Card validation

The **Unlock Card** workflow no longer requires any further additional authentication. Any operator with access to this workflow can unlock the cards of any user within their scope. On new installations, this workflow is assigned only to the Security Officer/Security Chief role. If you are upgrading to the current version, you are recommended to review the roles to which you assign this workflow to ensure that your system is set up to meet your security requirements.

Self-service card unlock using the **Reset PIN** option has been enhanced to enforce authentication methods configured in the credential profile used at issuance in addition to global configuration.

See the ***Administration Guide*** for details.

Note: As of MyID 10.7, **Unlock Card** has been replaced by **Reset Card PIN**.

14.7 Authenticating users

The **Authenticate Person** workflow allows a MyID operator to authenticate the identity of a cardholder using biometrics (if supported in your installation of MyID), identity documents, or operator approval. The authentication is recorded in the MyID audit trail.

This workflow allows you to carry out authentication when required to by your process; for example, for FIPS 201-2, you must confirm the identity of the cardholder before carrying out changes on their card.

See the ***Administration Guide*** for details.

14.8 Disposing of cards

You can mark a card as disposed within MyID. This creates an audit trail of the date and time of the disposal along with the identity of the operator who disposed of the card.

See the ***Administration Guide*** for details.

14.9 Improved envelope mechanism

MyID now has an improved envelope mechanism. This provides enhanced security for data transferred between MyID clients and the MyID server.

When you install MyID, it is configured to support the new Envelope Version 1.3 in addition to the previous Envelope Version 1.2.

- Windows clients (MyID Desktop, Self-Service App, and Self-Service Kiosk) that use MyID Client Components version UMC-10.1.1000.14 or later (as provided with MyID 10.1) support the new Envelope Version 1.3.
- Windows clients using older versions of the MyID Client Components support only the previous Envelope Version 1.2.
- Mobile clients support only the previous Envelope Version 1.2.

You can choose which envelope mechanisms to support in MyID.

To select the envelope mechanisms:

1. From the **Configuration** category, select **Security Settings**.
2. On the **Server** tab, set the following:
   - **Allow envelope version 1.2** – MyID allows clients to connect using the older envelope mechanism. All clients support this mechanism.

     You must select this option to allow mobile clients to connect to MyID.

     You must also select this option to allow the MyIDEnroll web service, which is used for the Lifecycle API, to operate correctly.
   - **Allow envelope version 1.3** – MyID allows clients to connect using the updated envelope mechanism. Windows clients using MyID Client Components UMC-10.1.1000.14 or later support this mechanism.

   Note: Do not deselect both options. If you deselect both options, no clients will be able to access MyID, and you will be locked out of the system. If you accidentally deselect both options, contact customer support, quoting reference SUP-140.
3. Click **Save changes**.

14.10 Mobile identities

This release provides further enhancements to the mobile capabilities of MyID. Supported platforms include Windows Phone 8.1, Android and iOS. See the ***Mobile Identity Management Installation and Configuration*** guide for further details.

Note: Additional updates are required to use this feature – contact Intercede quoting SUP-60 for further details.

Some of the features include the following:

- Ensure mobile credentials are only issued to known devices.

  This is a configurable option that enables organizations to control and manage the person and the device to which credentials are issued. This feature has several benefits including:
  - A mechanism which can be leveraged by Mobile Device Management (MDM) vendors to push registered mobile device details through to MyID such as serial number or hardware unique identifier.
  - Enablement of Bring Your Own Device (BYOD) corporate policy. This allows firms to manage credentials on mobile devices not issued by them including lifecycle management.

- Enhanced OTP delivery mechanism

  This function now allows the customer to configure how the OTP code is delivered to the mobile. This includes SMS delivery.

- Windows Phone

  Mobile credentials for Windows Phone 8.1 can now be fully managed through issuance, maintenance and termination stages of the lifecycle.

- Android Support

  Further enhancements to this platform include support for UICC (Gemalto PIV) credential store.

15 Previously in MyID 10.0

This section describes the changes that were made for the MyID 10.0 release.

15.1 Installation program

The installation program has been updated to provide a simpler installation process with support for Windows Server 2012 R2 and SQL Server 2012 SP1. You no longer need additional compatibility add-ons for database installation.

See the ***Installation and Configuration Guide*** for details.

15.2 Unique IDs for audit information and certificates

In previous versions of MyID, the logon name was used to link to audit information, jobs, and certificates which had the potential to cause problems if you changed the logon name or added a new user with a logon name that had been used by a now-deleted user.

From 10.0, this has been changed to a unique ID – this means that you can now change the logon name of a user, and the user will retain their certificates and maintain the link to their transactions in the audit trail.

If you are upgrading from a previous version of MyID, the installation program updates your certificates and job information. If you have a large system with many certificates or job records, this may take some time.

In the **Audit Reporting** workflow, the **Logon Name** field now returns the records for the unique user ID that matches the logon name – if you want to search for *all* audit records that used that logon name, including transactions that were audited against a previous logon name before you upgraded to the current version, or transactions for users that have been deleted, select the **Historic** option.

15.3 Device identities

You can now issue and manage certificates that represent the identity of a device rather than an individual person. In this release, you can issue a certificate to a computer containing a Trusted Platform Module (TPM), allowing authentication to your network infrastructure. The new Device Management API allows you to control the process through an external system, with a streamlined collection process on the computer.

See the ***Administration Guide*** for details of working with device identities, and the ***Device Management API*** document in the MyID Device Management API web service module for details.

15.4 Mobile identities

You can issue user authentication and encryption certificates to mobile devices such as Apple iOS and Android smartphones and tablets.

Issuance takes place over an Internet connection using the native certificate storage features of the mobile operating system.

Use of this feature requires an additional update to be installed. Contact Intercede if you are interested in using this capability.

15.5 Microsoft Virtual Smart Cards

You can issue and manager user certificates that are stored on a TPM-based virtual smart card (VSC), providing two-factor authentication and integration with Windows without physical smart cards.

See the ***Administration Guide*** for details of working with VSCs.

15.6 Self-Service applications

The Self-Service App is designed to run on an individual user's PC and prompt the cardholder when their device needs to be collected, activated or updated. It also issues and manages Microsoft Virtual Smart cards and device identities.

The Self-Service Kiosk is designed to run on a shared PC, for example in an entrance lobby or visitor desk, and allow any cardholder to collect, activate or update their devices, and to request and collect temporary or replacement devices.

See the ***Self-Service Installation and Configuration*** document in the Self-Service App module for details.

15.7 PIV card support

Previously limited to US Federal customers only, MyID can now support PIV cards for all installations. This allows use of NIST approved smart cards with direct-to-card-edge integration, so no additional middleware is required. GlobalPlatform key management, multi-stage issuance models, and secure activation processes are also now available.

Note: This feature allows you to use PIV smart card technology, but does not provide the issuance process or trust level that meets NIST standard FIPS-201. If you want to issue credentials that meet FIPS-201 requirements, contact Intercede to discuss this further.

See the ***Smart Card Integration Guide*** for details.

15.8 Updated printer support

For Fargo printers, this release provides more advanced control of card printers using the Fargo SDK and simpler integration for a wider range of models.

For Zebra printers, this release provides support for the ZXP-7 and ZXP-8 models.

See the ***Printer Integration Guide*** for details.

15.9 Global key recovery

You can now allow all encryption certificates belonging to a user to be recovered automatically the next time a card is issued.

See the **Global Historic Certificates** option in the ***Administration Guide*** for details.

15.10 File storage in the database

Images and other files can now be stored in the database as binary objects; previously, images were stored on the web server in the `upimages` folder. This improves security and increases your options for carrying out backups. You can configure additional security restrictions to restrict access to images to specified user roles.

15.11 Terminology updates

Some of the terminology used in MyID has changed to reflect the broader range of features introduced for mobile and device identities; for example, card profiles are now known as credential profiles.

See the *Terminology* section in the ***Administration Guide*** for details of the terminology used in the current version.

15.12 Combination of documentation

The structure of the documentation has been updated to include fewer volumes.

- The ***Administration Guide*** now contains the content from both the ***Administration Guide*** and the ***User Guide***.
- The ***Installation and Configuration Guide*** now contains the content from the ***Installation and Configuration Guide***, ***Hardware and Software Requirements Guide***, ***Getting Started***, ***Business Continuity Planning***, ***Failover Strategy*** and ***Advanced Deployment***.

This change is designed to make it easier to find the information you need.

15.13 End of life features

The following features became no longer supported in MyID effective with version 10.0.

15.13.1 Online help

The online help, which previously contained a cut-down copy of the procedural information from the ***User Guide*** and the ***Administration Guide***, has been removed from the web user interface. The product documentation will be updated and released more frequently, and this is now the source of user information.

15.13.2 List Devices workflows

The **List Devices** and **List Devices (Admin)** workflows have been removed. You can use the **MI Reports** workflow to produce a list of the issued smart cards.

15.13.3 MIFARE

If you want to use MyID to write data to MIFARE cards, contact customer support for more information, quoting reference SUP-97.

15.13.4 Import from file

You can no longer import user account data using XML file upload. To import user account data, use directory integration or the Lifecycle API.

15.13.5 SMTP email

You must use the Database Mail feature of SQL Server for all email notifications. The older method of using XPSMTP is no longer supported in SQL Server.

See the ***Installation and Configuration Guide*** for details of setting up Database Mail.

15.13.6 Smart card support in GenMaster

GenMaster no longer provides the ability to store master keys on a smart card. You can store your master keys in the registry or on an HSM.

If you currently use a smart card to store your master keys, you are recommended to switch to storing your keys on an HSM. Contact Intercede to discuss this further before upgrading your installation.

You no longer need to use GenMaster to create administrator cards. Instead, you can use GenMaster to set the password for the startup user. You can then use this startup user to access MyID and create further operator accounts.

15.13.7 Soft certificates

You can no longer use the **Request Soft Certificates** and **Issue Soft Certificates** workflows to request or issue soft certificates. Instead, you can create a credential profile to issue the certificates.

See the ***Administration Guide*** for details.

15.13.8 Request and collect certificate recovery

You can no longer use the **Request Certificate Recovery** and **Collect Certificate Recovery** workflows to carry out multi-stage key recovery.

This feature is replaced by the Key Recovery workflows – see the ***Administration Guide*** for details.

15.13.9 Windows XP for client PCs

Microsoft Windows XP is no longer supported for new installations of MyID, as Microsoft have now officially ended support for this operating system. If you are upgrading from an existing version of MyID, and still require the use of Windows XP, contact customer support for more information quoting reference SUP-108.

16 Previously in Mobile Releases

Releases before MyID 10.6 contained features for mobile identity management in a separate module.

16.1.1 MOB-10.5.1000.1

Release MOB-10.5.1000.1 contained the following change:

- Error logging.

  This release includes the ability to log errors (for example, errors caused by infrastructure or connectivity failures) during the certificate provisioning process. Log files can then be emailed to an administrator for diagnosis and more rapid troubleshooting.

  See the ***Mobile Identity Management Installation and Configuration Guide*** and ***Derived Credentials Installation and Configuration Guide*** for details.

16.1.2 MOB-10.4.1000.1

Release MOB-10.4.1000.1 contained the following changes:

- Wider range of supported mobile devices. See the ***Mobile Identity Management Installation and Configuration Guide*** for details.
- **Important:** The process for issuing credentials to mobile devices has been improved. For further details about configuring and issuing mobile credentials, see the ***Mobile Identity Management Installation and Configuration Guide***.
- Historic certificates support for mobile devices

  MyID now has the ability to share encryption certificates across multiple devices, allowing the recovery of archived certificates issued to a smart card and the delivery to a mobile device through the provisioning process.

  In practice, this means that a user can send an encrypted email using their smart card on their workstation in the office, and while on the move can use their mobile device to decrypt the email.

  Also, users can now decrypt emails from their mobile device including those where certificates may have expired.

- User defined certificate names

  Users can now specify meaningful names for certificates provisioned both on their mobile devices and on other credentials such as a smart card when used with the mobile device. User-friendly names are saved and displayed on the mobile device's certificate list when authentication is required and are maintained throughout the certificate renewal process.

- Mobile integration with Citrix

  MyID can now provision credentials to a mobile device enrolled into the Citrix XenMobile environment. The credentials are delivered to a secure Citrix Certificate Vault which enables Citrix Ready Worx verified apps to consume those credentials. This means the Citrix customer base can use WorxMail for signing and encrypting emails on the mobile device.

- Improvement to mobile provisioning process

  The process for issuing credentials to mobile devices has been improved. A trust anchor is no longer required for the provisioning process to complete successfully. Previously, this was based on delivering a certificate using a PFX file to the mobile. Other changes include a simplified audit trail and some elements of configuration.

16.1.3 MOB-10.3.1000.2

Release MOB-10.3.1000.2 contained the following changes:

- Updated documentation to match new versions of MyID Web Services and Client Components.

16.1.4 MOB-10.3.1000.1

Release MOB-10.3.1000.1 contained the following changes:

- Support for separate workflows for derived credentials for known and unknown cards.
- Removal of the need to use a Virtual Smart Card (VSC) for derived credentials.

16.1.5 MOB-10.1.1000.2

Release MOB-10.1.1000.2 contained the following changes:

- MOB-10.1.1000.1 was restricted to only 10.1 MyID systems. The current release of the patch contains bug fixes.
- Support for issuing certificates to Android phones into the Java KeyStore.

16.1.6 MOB-10.1.1000.1

Release MOB-10.1.1000.1 contained the following changes:

- Support for MyID version 10.1.
- Device registration.

  You can use the **Mobile Device Restrictions** option to set up your credential profiles to issue mobile identities only to those mobile devices that have been registered with MyID.

  See the *Registering devices* section of the ***Mobile Identity Management Installation and Configuration Guide***.
- Support for Windows phone.
- Support for derived credentials.

  You can now issue mobile identity that is based on an already-issued credential – the mobile identity is derived from the previously-issued credential.

  See the ***Derived Credentials Guide*** for details.
- Issuing OTP authentication codes by SMS

  You can now choose to send OTP authentication codes directly to the appropriate mobile device rather than displaying the codes on the operators' screens. See the *Configuring SMS and email notifications* section of the ***Mobile Identity Management Installation and Configuration Guide***.
- Issuing soft certificates

The ***Software Certificates for iOS and Android Installation and Configuration Guide*** is no longer provided with this release. You can now request soft certificates for Android and iOS using **Request ID** or **Request My ID**.

16.1.7 MOB-10.0.1000.5

Release MOB-10.0.1000.5 contained the following change:

- Support for collecting soft certificates using the Identity Agent app on Android.

16.1.8 MOB-10.0.1000.4

Release MOB-10.0.1000.4 contained the following changes:

- You can now manage mobile identities on Windows Phone 8.1 devices with a TPM virtual smart card.
- Provisioning mobile identities on iOS to the Intercede keystore is now accompanied by optional identity badge layout screens.

16.1.9 MOB-10.0.1000.2

Release MOB-10.0.1000.2 contained the following change:

- You can now manage mobile identities on iOS with an attached iCarte sleeve.

16.1.10 MOB-10.0.1000.1

Release MOB-10.0.1000.1 contained the following changes:

- You can now manage mobile identities on iOS and Android mobile devices as well as BlackBerry smartphones.
- The workflows used to manage mobile identities have changed, and are now grouped under the **Mobile Devices** category within MyID.
- The ***Mobile Identity Management for BlackBerry Smartphones Configuration Guide*** has been renamed the ***Mobile Identity Management Installation and Configuration Guide***.
- The ***Mobile Identity Management Installation and Configuration Guide*** previously issued in patch P901MP164 has been renamed the ***Software Certificates for iOS and Android Installation and Configuration Guide***.

17 Known Issues

- **IKB-15 – Problems collecting or updating cards**

  If you experience problems when collecting or updating cards, try increasing the **Certificate Refresh Threshold** option on the **Certificates** tab of the **Operation Settings** workflow to a higher value; for example, `45`.

  This problem may manifest with an error similar to:

  ```
  One of the certificates that have been requested for you has failed
  to issue. Please contact your administrator.
  ```

  Note that the certificate may have issued correctly even though the card update has failed.

- **IKB-16 – Pressing back shortcut key causes blank screen**

  As many MyID workflows are based on web pages, and MyID Desktop embeds Internet Explorer to display these workflows, you may experience problems if you attempt to use the browser's controls to go back; for example, pressing ALT + left arrow or pressing Backspace when not editing a field. These browser controls cannot be overridden.

  Typically, the problem presents itself as a blank screen.

  If this happens, click the Home button and restart the workflow.

- **IKB-20 – Pressing refresh (F5) causes blank screen**

  As many MyID workflows are based on web pages, and MyID Desktop embeds Internet Explorer to display these workflows, you may experience problems if you attempt to use the browser's controls to refresh the screen using the F5 key.

  Typically, the problem presents itself as a blank screen.

  If this happens, click the Home button and restart the workflow, or close MyID Desktop and restart.

- **IKB-27 – Cannot click on links in email notifications**

  There is an issue with links being removed from email messages. This may occur with emails received through Outlook Web Access or on some mobile mail clients. In some cases, Microsoft Exchange may remove hyperlinks from messages.

  For more information, contact Intercede customer support quoting reference SUP-176.

- **IKB-35 – OTP fails to validate if security phrases are locked**

  If you attempt to validate a job OTP (for example, a logon code, or a challenge code for SCEP issuance) but the user's security phrases are locked, the validation will fail.

  As a workaround, unlock the user's security phrases using the **Unlock Security Phrases** workflow before attempting to validate the OTP.

- **IKB-80 – Cannot activate a card that has been reinstated when it was issued using 1-Step pre-encoding**

  If you have issued a card using the **1-Step** option for **Pre-encode Card** in the credential profile, then use **Reinstate Card**, you cannot proceed to activate the card; the card is not recognized as being ready for activation.

  As a workaround, you must cancel and re-issue the card.

- **IKB-81 – Cannot click on links in email notifications**

  You can configure MyID to notify users by email that a mobile identity is available for them to collect. There is an issue with some email servers where they remove links from email messages before sending the message to mobile clients, which stops the email notification link from being used to start Identity Agent to collect the mobile identity. Additionally some email clients can also remove the link even if it has been provided in the email from the server. For more information, contact Intercede customer support quoting reference SUP-176.

- **IKB-84 – Cannot use the Request Replacement ID workflow with Identity Agent-based credential profiles**

  The **Request Replacement ID** workflow allows you to request a replacement ID for a user where the mobile device may have been lost or stolen. If the credential profile used to issue the mobile ID had the **Identity Agent (Only)** option selected, you cannot use this workflow; an error appears in MyID when you attempt to request a replacement ID.

  As a workaround, you can cancel the mobile credential using the **Cancel Credential** workflow, then request a new mobile identity for the user.

- **IKB-88 – Existing mobile credentials overwritten**

  When using Identity Agent-based credential profiles, if you request a mobile identity for a user, the new identity overwrites the existing identity; the original identity is cancelled in MyID, but the certificates remain issued.

- **IKB-118 – Issue when using MyID Desktop with JAWS**

  You may experience an intermittent problem when using the JAWS screen-reading software (version 12 and later): MyID Desktop may become unresponsive when you open the New Action dialog, depending on the number of available workflows.

- **IKB-179 – Cannot request an authentication code to unlock a mobile device**

  The **Unlock Credential** workflow can require an authentication code to confirm the user's identity before proceeding with the unlock process. For mobile credentials, it is not currently possible to request an authentication code for unlocking. Ensure that operators who perform unlock for mobile devices do not require authentication codes, or can bypass authentication where needed.

- **IKB-182 – Mobile devices with multiple keystores show one entry, but cancel all**

  When canceling credentials on a mobile device, the search results display a single entry that represents the primary keystore on the device. Where the device has been issued with multiple keystores, all the associated certificates will be canceled.

- **IKB-215 – Software certificate renewals use the original credential profile settings**

  The content of software certificate packages is determined by a credential profile. When renewing software certificates, changes to the certificate policies assigned to the credential profile will not be picked up – the policies defined in the original version of the credential profile will be used. If a certificate policy has been superseded, the replacement policy will be used automatically.

- **IKB-219 – Contactless card detection**

  There are some differences between the **Issue Card** workflow and the updated **Collect Card** and **Batch Collect Card** workflows.

  With **Issue Card**, you cannot issue a dual-interface (contact chip and contactless) smart card unless it has been previously imported to the system using the **Import Serial Numbers** workflow, or it has been previously issued as a dual-interface smart card using **Collect Card**. Unknown dual-interface cards are not supported. Contactless-only cards require the credential profile to be set as **Must be a Proximity Card** when used with **Issue Card**.

  If you require Contactless-only card issuance to be restricted to known devices only (to enforce the credential profile setting **Must be a known Proximity Card**), or require information to be sent to a PACS, the card details must be imported separately. Contact customer support quoting reference IKB-219 for assistance.

- **IKB-222 – Entrust integration not available on Windows Server 2016**

  At the time of release, integration of MyID with Entrust PKI is not available for MyID application servers running on the Windows Server 2016 operating system, due to dependencies on required Entrust components. Contact customer support quoting reference IKB-222 for further details.

- **IKB-236 – Differences in PIN policy between Change PIN and Reset PIN workflows**

  You can set the PIN Policy for smart cards within the credential profile. If you change the PIN policy in the credential profile after issuing a card, the **Change PIN** workflow, and older web-based workflows (**Unlock Card**, **Auto Unlock Card**) will continue to use the PIN policy set at the time the card was issued.

  The Self-Service Kiosk, the **Reset Card PIN** workflow, and self-service **Reset PIN** feature in MyID Desktop will use the PIN policy from the latest version of the credential profile, allowing PIN policy to be changed at any time. During any issuance process, the PIN policy is always taken from the latest version of the credential profile.

  If you need to modify your PIN policy and are affected by this issue, please customer support quoting reference SUP-284.

- **IKB-237 – Security question authentication fails when the user logon name contains an apostrophe**

  Security question authentication fails for users who have an apostrophe character in their MyID logon name. This field may have been imported to MyID from an Active Directory attribute or the Lifecycle API, or been set manually by a MyID operator.

  Security question authentication can be used during logon to MyID, the self-service **Reset PIN**, **Authenticate User** and **Reset Card PIN** workflows in MyID Desktop, or authentication during card collection processes in the MyID Self-Service App.